

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002 年 5 月 16 日 (16.05.2002)

PCT

(10) 国際公開番号
WO 02/39294 A1(51) 国際特許分類⁷: G06F 15/00, H04Q 7/38, H04L 9/32

(21) 国際出願番号: PCT/JP01/09780

(22) 国際出願日: 2001 年 11 月 8 日 (08.11.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

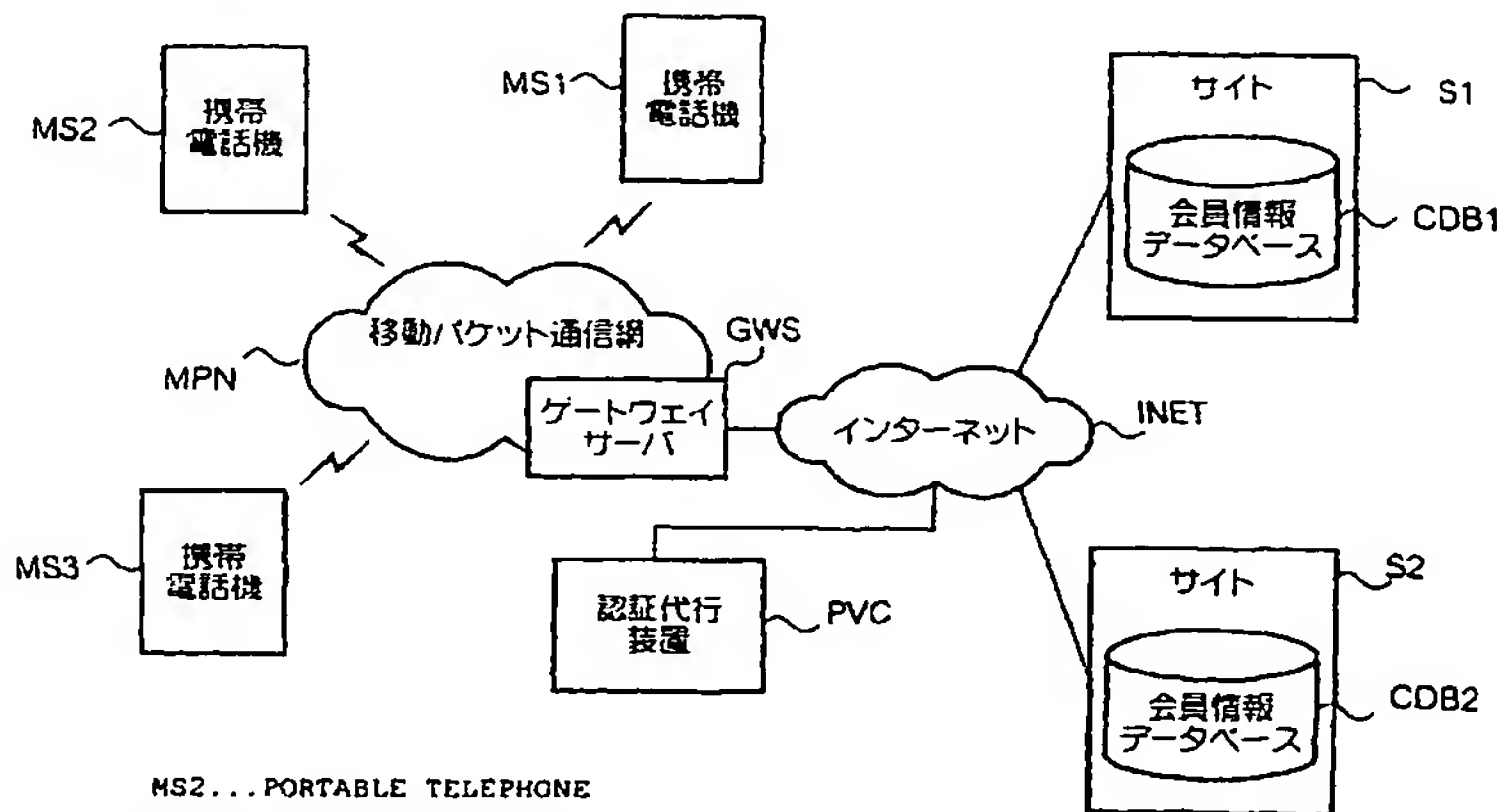
(30) 優先権データ:
特願 2000-344402
2000 年 11 月 10 日 (10.11.2000) JP(71) 出願人 (米国を除く全ての指定国について): 株式会社
エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.)
[JP/JP]; 〒100-6150 東京都千代田区永田町二丁目 11
番 1 号 Tokyo (JP).(71) 出願人 (日本についてのみ): 株式会社 アニモ (ANIMO
LIMITED) [JP/JP]; 〒231-0015 神奈川県横浜市中区尾
上町二丁目 27 番 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 夏野 剛 (NAT-
SUNO, Takeshi) [JP/JP]; 〒153-0062 東京都目黒区三
田一丁目 5-6 1002 号 Tokyo (JP). 桑名隆滋 (KUWANA,
Ryuji) [JP/JP]; 〒231-0015 神奈川県横浜市中区尾上町
二丁目 27 番 株式会社 アニモ内 Kanagawa (JP).(74) 代理人: 川崎研二 (KAWASAKI, Kenji); 〒103-0027 東
京都中央区日本橋一丁目 2 番 10 号 東洋ビルディング
7 階 朝日特許事務所 Tokyo (JP).(81) 指定国 (国内): AU, BR, CA, CN, JP, KR, NO, NZ, PL,
SG, US.(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE,
DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).添付公開書類:
— 国際調査報告書2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

(54) Title: AUTHENTICATION SYSTEM, AUTHENTICATION AGENT APPARATUS, AND TERMINAL

(54) 発明の名称: 認証システム、認証代行装置および端末装置



MS2...PORTABLE TELEPHONE
MS1...PORTABLE TELEPHONE
MPN...MOBILE PACKET COMMUNICATION NETWORK
MS3...PORTABLE TELEPHONE
GWS...GATEWAY SERVER
PVC...AUTHENTICATE AGENT APPARATUS
INET...INTERNET
S1...SITE
CDB1...MEMBER INFORMATION DATABASE
S2...SITE
CDB2...MEMBER INFORMATION DATABASE

(57) Abstract: An authentication system has a communication network, terminals, and an authentication agent apparatus. The authentication agent apparatus authenticates a user by using information including at least information fixed to a terminal or information unique to the user of a terminal, specifies a site that user desires, references the database containing authentication information needed when the user is to use the desired cite after authenticated, and agents for the authentication.

[続葉有]

WO 02/39294 A1



(57) 要約:

認証処理システムが、通信網と複数の端末装置と認証代行装置を有する。
認証代行装置は、端末装置に固定された情報あるいは端末装置の利用者に固有の情報の少なくとも一つを含む情報を利用して利用者を認証し、利用者が希望するサイトを特定して、認証された利用者が希望するサイトを利用する時に必要となる認証情報を格納しているデータベースを参照して認証処理を代行する。

明 細 書

認証システム、認証代行装置および端末装置

5 技術分野

この発明は、通信網を介して会員にサービスを提供するサイトへ、会員の認証に必要な認証情報を渡すことで、端末装置を使用する会員による認証情報の手動入力を排除する認証システムと、この認証システムを構成する認証代行装置および端末装置に関する。

10

技術背景

インターネットの普及とともに、インターネットを介して、限定された会員にサービスを提供する会員制インターネット・サイトや利用者毎に内容の異なるサービスを提供するサイト（これらを、以降、会員制サイトあるいはサイトと称す。）が現われてきている。これらのサイトの運営者は、登録会員あるいは登録利用者（以降、会員と称す。）に対して固有のID（識別情報）とパスワード（このIDとパスワードをまとめて、これ以降、個別認証情報と称す。）を発行する。

ある会員が、あるサイトの提供するサービスを端末装置から利用しようとする時に、当該サイトは、当該会員の使用する端末装置に個別認証情報の入力フォームを送信して、個別認証情報の入力を要求する。当該会員は、この入力要求に対して、端末装置を操作して、個別認証情報を手動で入力する。当該サイトは、この個別認証情報を受信し、受信した個別認証情報が正しい場合に、この端末装置からのサービス利用要求が会員等からの利用要求であると認証する。認証された端末装置を使用する利用者は、以降、このサイトが提供する所望のサービスを利用することができる。

このような会員制サイトを複数利用する端末装置の利用者は、各々のサービスを利用するために、それぞれのサービスに対応した複数の個別認証情報を記憶する必要があった。複数のサービスに使用する個別認証情報を共通の

ものとすることができれば、利用者の記憶の問題は解決できるかもしれない。

しかし、実際には、個別認証情報の形式や属性は統一されていないから、サイト毎に異なっていることが多い。例えばあるサイトの個別認証情報は4～8文字からなる数字のみのIDと8～12文字からなる英字のみのパスワードからなり、別のサイトの個別認証情報は9～10文字の英数字からなるIDのみからなるということがある。また、サイトの個別認証情報を会員が自由に選択できない場合も多い。さらに、複数のサイトの個別認証情報を共通にすることはセキュリティの観点からも好ましくない。したがって、個別認証情報の共通化による個別認証情報の集約は困難であった。

10 たとえば個別認証情報の共通化ができた場合であっても、会員制サイトを利用する時に個別認証情報を手動で入力しなければならない点は不便なままであり、解決されていない。たとえば、端末装置の使用者が個別認証情報を入力して、ある会員制サイトのサービスを利用した後に、個別認証情報が共通している別の会員制サイトのサービスを利用するときに、個別認証情報をも
15 う一度入力する必要があった。

個別認証情報の入力を省略する利用者にとって利便性の高い方法がある。

第1の例として、端末装置が個別認証情報の入力フォームを受信した時に、該当する入力フィールドに個別認証情報を自動入力させる方法がある。このようにすれば端末装置の使用者が個別認証情報を入力する手間を削減すること
20 ができる。

しかし、この場合、個別認証情報が端末装置に記憶されていることになるから、この記憶されている個別認証情報が、第3者の手に渡って悪用されるおそれがある。また、セキュリティの観点からこの方法は好ましくない。

第2の例として、グローバルIDサービスと呼ばれるサービスがある。

25 このサービスは、利用者に、利用する複数の会員制サイトの個別認証情報をこのサービスを提供するサイトに格納しておくこと手段を提供している。このサービスの利用者は、インターネットを介して当該サイトに、IDとパスワードを入力してログインした後は、当該サイトが、当該利用者が利用しようとする会員制サイトからの要求を満たす個別認証情報を、個別の会員制

サイトに提供する。すなわち、このサービスの利用者は会員制サイト毎に個別認証情報を手動で入力する必要がなくなる。

- しかし、グローバルサービスにログインするために必要なIDおよびパスワードが漏洩すると、当該サイトに格納されている全ての個別認証情報がま
5 とまって漏洩することになる。すなわち、グローバルIDサービスを使うことにより、使用者が複数の個別認証情報を管理するよりも、個別認証情報の漏洩の危険性が増大することになるという問題があった。

発明の開示

- 10 本発明は、通信網と、前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、前記サイトに入力するに
入力する個別認証情報を前記端末装置の使用者に対応して格納した第1のデータベースと、前記端末装置の使用者を当該端末装置に固定された
15 情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する認証手段と、前記認証手段により認証された使用者が利用を希望するサイトを
特定する特定手段と、第1のデータベースを参照して前記手段により認証された使用者と前記特定手段により特定されたサイトに対応した個別認証情報を
抽出して、当該サイトに抽出された個別認証情報を渡す代行手段とを有し、
前記通信網に接続した認証代行装置とを有する認証処理システムを提供する。

- 20 また、本発明の認証処理システムは、生体に固有な情報を使用して前記端末装置の使用者を認証することが好ましい。さらに、取得した生体に固有な情報の
認証前段処理手段を有する前記端末装置を備えることがより好ましい。

- また、本発明の認証処理システムは、前記使用者が認証レベルの選択を可能とする認証レベル選択手段を備えていることが好ましい。さらに、前記認
25 証レベルに基づいて保険料を決定する保険料請求手段を供えていることがより好ましい。

また、本発明の認証処理システムは、認証の効果の有効期限を管理する認証有効期限管理手段を備えていることが好ましい。

また、本発明の認証システムは、前記第2のデータベースを、前記複数の

サイトが更新することを可能とする更新手段を備えていることが好ましい。

本発明の認証代行装置は、サイトに入力する個別認証情報を端末装置の使用
者に対応して格納した第1のデータベースと、前記端末装置の使用者を当
該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一
5 方を利用して認証する認証手段と、前記認証手段により認証された使用者が
利用を希望するサイトを特定する特定手段と、第1のデータベースを参照し
て前記手段により認証された使用者と前記特定手段により特定されたサイト
に対応した個別認証情報を抽出して、当該サイトに抽出された個別認証情報
を渡す代行手段とを備える。

10 また、本発明の認証代行装置は、生体に固有な情報を使用して前記端末装
置の使用者を認証することが好ましい。

本発明の端末装置は、通信網に接続することができる通信手段と、前記通
信網を介してサイトおよび認証代行装置に接続することができる接続手段と、
生体に固有な情報を取得する手段と、取得した生体に固有な情報を認証前段
15 処理する手段を備える。

図面の簡単な説明

図1は、本発明の第1および第2の実施形態に係る認証システムの構成
を示すブロック図である。

20 図2は、第1および第2の実施形態に係る認証代行装置PVCの構成を示
すブロック図である。

図3は、認証用データベースVDB内の個人用テーブルT1の構成を例示
する概念図である。

図4は、サイト情報データベースSDB内のサイト別テーブルT2の構成
25 を例示する概念図である。

図5は、第1および第2の実施形態に係る形態に係る携帯電話機MSの構
成を示すブロック図である。

図6は、携帯電話機MSが備える決定ボタン41の概念図である。

図7は、携帯電話機MS2に表示される画面例を示す図である。

図 8 は、第 1 の実施形態に係る携帯電話機 M S 2 の使用者が会員登録を行う場合の情報の流れを示す図である。

図 9 は、第 1 および第 2 の実施形態に係る携帯電話機 M S が H T M L データ中に認証情報の入力タグが含まれた場合に行う処理の流れを示すフローチャートである。

図 1 0 は、第 1 の実施形態に係る携帯電話機 M S 2 の使用者がメニュー登録を行う場合の情報の流れを示す図である。

図 1 1 は、第 1 の実施形態に係る認証代行装置 P V C が行う認証代行処理の流れを示すフローチャートである。

10 図 1 2 は、第 1 の実施形態に係る認証サービスを携帯電話機 M S 1 の使用者が利用する場合の情報の流れを示す図である。

図 1 3 は、携帯電話機 M S 1 に表示される画面例を示す図である。

図 1 4 は、第 1 の実施形態の認証サービスでおこなわれる認証処理を示す概念図である。

15 図 1 5 は、第 1 の実施形態に係る認証サービスを携帯電話機 M S 1 の使用者が複数のサイト S 1、S 2 に利用する場合の情報の流れを示す図である。
認証代行装置 P V C が行う認証代行処理の流れを示すフローチャートである。

図 1 6 は、携帯電話機 M S 3 の使用者が認証代行サービスを受けようとした場合の情報の流れを示す図である。

20 図 1 7 は、携帯電話機 M S 3 に表示される画面例を示す図である。

図 1 8 は、本実施形態に係る認証システムの認証レベルを示す図である。

図 1 9 は第 2 の実施形態に係る認証サービスを携帯電話機 M S 1 の使用者が利用する場合の情報の流れを示す図である。

25 発明を実施するための最良の形態

本発明をより詳細に説明するために、添付の図面に従ってこれを説明する。

< A. 第 1 実施形態 >

< A - 1. 構成 >

< A - 1 - 1. 概要 >

図1は、本発明の第1の実施形態における認証システムの構成を示すブロック図である。同図に示すように、本実施形態における認証システムは、認証代行装置PVC、複数の携帯電話機MS（MS1～MS3）、複数の会員制サービス提供サイトS（S1～S2）、移動通信網MPN、インターネットINET、
5 およびゲートウェイサーバGWSを有する。

本実施形態における認証システムに収容可能な携帯電話機MSの数は任意であり、携帯電話機MSの数は図示されている数に限定されない。本実施形態における認証システムに収容可能なサイトSの数は任意であり、サイトSの数は図示されている数に限定されない。

10 認証代行装置PVCは、インターネットに接続されている。認証代行装置PVCは、携帯電話機MSの使用者が会員制サービス提供サイトS（S1～S2）の利用を開始する際に当該利用者がおこなう処理を代行する（認証代行処理と称す。）サービスを提供する。この認証サービスは会員制のサービスである。認証代行装置PVCは、当該サービスの会員に会員番号を与え、
15 会員に全体認証情報を登録することを要求する。

携帯電話機MS（MS1～MS3）は、それぞれ移動通信網MPNに無線通信で接続することができる。

会員制サービス提供サイトS（S1～S2）は、インターネットに接続されている。サイトS（S1、S2）は、インターネットの利用者に対して会
20 員制サービスを提供する。サイトS（S1、S2）は、サービスを利用する会員を認証するための個別認証情報を格納した会員情報データベースCDB（CDB1、CDB2）を有する。サイトSは会員情報データベースに登録された会員にのみサービスを提供する。この個別認証情報は、会員番号（会員ID）および認証情報（パスワード）を含む。

25 本実施形態におけるサイトS1は、SSL（Secure Sockets Layer）暗号化プロトコルを利用した通信（SSL通信と称す）を利用できる会員にのみ、会員制サービスを提供している。

移動通信網MPNは、複数の基地局、複数の交換局、複数の関門中継交換局、複数の加入者処理装置、ゲートウェイサーバGWS、ならびにこれらを

接続する無線および有線通信回線を備えている。移動通信網M P Nは、携帯電話機M S使用者に、携帯電話機M SとインターネットI N E Tとの間を中継する機能と当該移動通信網の利用料金を当該使用者に請求する機能を有する。

- 5 ゲートウェイサーバG W Sは、移動通信網M P NとインターネットI N E Tを含む他のネットワークとを、ネットワーク間で異なる通信プロトコルの変換を行うことにより、相互接続する。ゲートウェイサーバG W Sは、移動通信網の関門中継交換局に備えることが好ましい。ゲートウェイサーバG W Sは、携帯電話機M SからH T T P (HyperText Transfer Protocol) プロト
10 コルのG E T要求（以降、G E T要求と称す）を受け取ると、当該G E T要求に含まれるU R I (Uniform Resource Identifiers) を解析する。ゲートウェイサーバG W Sは、当該U R Iが、インターネットI N E T上を指し示す場合に、インターネットI N E Tへ当該G E T要求を転送する。ゲートウェイサーバG W Sは、インターネットI N E Tから送信されてきた当該G E
15 T要求に対する応答を受信する。ゲートウェイサーバG W Sは、当該応答を携帯電話機M Sに送信する。

また、ゲートウェイサーバG W Sは、当該U R Iが自己のリソースを示す場合には、当該G E T要求に対応するリソースを、携帯電話機M Sに送信する。ゲートウェイサーバG W Sが保有するリソースは、H T M L (HyperText
20 Markup Language) 形式で記述された携帯電話機M Sのユーザインタフェースを定義するU I 定義情報を含む。

しかし、ゲートウェイサーバG W Sは、携帯電話機M Sがインターネットのあるサイトと、S S L暗号化プロトコルを利用したH T T P通信をしている時 (https://で指定された場合) は、携帯電話機M Sと当該サイトの間の
25 通信内容に関与しない。

< A - 1 - 2 . 認証代行装置 >

図2は、本実施形態における認証代行装置P V Cの構成を示すブロック図である。この図に示すように、本実施形態における認証代行装置P V Cは、

認証用データベースVDB、サイト情報データベースSDB、通信部P1、操作部P2、表示部P3、記憶装置P4および制御部P5を有する。

5 認証用データベースVDBは、さらに個人用テーブルT1を有する。図3は、個人用テーブルT1の構成を示す概念図である。同図に従って個人用テーブルT1について説明する。

個人用テーブルT1には、認証サービスの会員ごとにレコードが設けられている。各レコードは、固有の会員番号を記憶する会員番号フィールド、当該会員の呼称（名前）を記憶する名前フィールド、当該会員が使用する携帯電話機MSの電話番号を記憶する電話番号フィールド、当該会員の認証（全体認証と称す）の基準となる情報（全体認証基準情報と称す）を暗号化して記憶する全体認証情報フィールド、認証レベルフィールド、全体認証の有効期限を記憶する有効期限フィールド、認証サービスの対象となる接続先のIDを記憶する接続先IDフィールド、接続先に入力する個別認証情報を暗号化して記憶する個別認証情報フィールド、第3者による不正利用に対する保険料を記憶する保険料フィールド、認証サービスの使用料を記憶する使用料フィールドを有する。

さらに、個人用テーブルT1は、当該会員が利用する複数の接続先に対応して、複数の接続先IDフィールドおよび当該接続先に対応した個別認証情報フィールドを有する。全体認証情報フィールドは、声紋情報フィールドと指紋情報フィールドにさらに分かれている。個別認証情報フィールドは、IDフィールドとパスワードフィールドにさらに分かれる。

これらのフィールドのうち、会員番号、呼称（名前）、携帯電話機MSの電話番号、当該会員の全体認証基準情報は、保険料、使用料の各フィールドには、会員登録時に、情報が格納される。

25 サイト情報データベースSDBは、さらにサイト別テーブルT2を有す

図4は、サイト別テーブルT2の構成を示す概念図である。同図に従ってサイト別テーブルT2について説明する。

サイト別テーブルT2は、接続先ID毎にレコードを設ける。各レコードは、接続先IDフィールド、接続先のタイトル名を格納するタイトルフィー

ルド、URIを含む接続するため情報を記憶する接続情報フィールド、提供するサービスの分類フィールド、当該サービスを利用するためにIDの入力を要するか否かを示すID要否フィールド、当該サービスを利用するためにパスワードの入力を要するか否かを示すパスワード要否フィールド、IDの入力を要する場合にはその属性（例えばバイト数）を記憶するID属性フィールド、パスワードの入力を要する場合にはその属性（例えばバイト数）を記憶するパスワード属性フィールドを有する。ここでID属性あるいはパスワード属性は、各会員制サービスが認証時に要求する個別認証情報に使用できる文字数、使用できる文字の種類を含む形式的要件である。さらに、図8
5 3の個人用テーブルT1と図4のサイト別テーブルT2は、接続先IDをキーとして関連付けられている。

通信部P1は、インターネットINETを介して他のノードと通信をすることができる。

操作部P2は、キーボード、ポインティングデバイスを備える。さらに操作指示やデータの输入のために使用する任意の装置を備えることができる。
15

表示部P3は、ディスプレイを備える。さらに任意の表示装置を備えることができる。

外部記憶装置P4は、電子ディスクやハードディスクを備える。さらに任意の外部記憶装置を備えることができる。

20 制御部P5は、CPU（Central Processing Unit）52と、インタフェースP51と、ROM（Read Only Memory）53と、RAM（Random Access Memory）54とを有する。

インタフェースP51は、CPU52と各部VDB、SDB、P1～P4を接続する。

25 CPU52は、インタフェースP51を介して各部VDB、SDB、P1～P4を制御して、認証代行装置PVCに、起動処理<A-2>、通信処理<A-3>、会員登録処理（<A-4-3>）、メニュー登録処理（<A-5-3>）、認証代行処理（<A-6-3>および<A-6-B>）、保険・課金処理（<A-7>）、サイト登録処理（<A-8>）を含む処理を実行

させる。各処理については後述する。

ROM 5 3 は、CPU 5 2 が上記の各処理を実行するソフトウェア、CPU 5 2 が参照する各種データならびにその他のソフトウェアおよび情報を記憶する。

5 RAM 5 4 は、CPU 5 2 のワークメモリとして使用される。

本実施形態における認証代行装置 P V C は、任意の数の CPU を有することができる。本実施形態における認証代行装置 P V C は、図 2 に示すように 1 CPU を有する装置で集中処理をしてもよいし、複数の CPU を有する装置で分散処理をしてもよい。

10

< A - 1 - 3 . 携帯電話機 M S >

図 5 は、本実施形態における携帯電話機 M S の 1 構成を示すブロック図である。同図に示すように、携帯電話機 M S は、通信部 1 、音響出力部 2 、音響入力部 3 、操作部 4 、表示部 5 および制御部 6 を有する。

15 通信部 1 は、無線通信を行うための、アンテナ、送信機および受信機を備える。通信部は移動通信網と無線通信をおこなうことができる。音響出力部 2 は、音源、スピーカおよび音を発するための装置を備える。

音響入力部 3 は、音声を入力するためのマイクを備える。

20 操作部 4 は、指示やデータの入力のためのキーパッド（図示しない）と、各種選択のためのボタン（図示しない）および決定ボタン 4 1 を備える。

表示部 5 は、表示するための液晶ディスプレイを備える。

制御部 6 は、インタフェース 6 1 と、CPU 6 2 と、ROM 6 3 と、フラッシュメモリ 6 4 および RAM 6 5 を有する。

インタフェース 6 1 は、CPU 6 2 と各部 1 ～ 5 を接続する。

25 CPU 6 2 は、インタフェース 6 1 を介して各部 1 ～ 5 を制御して、携帯電話機 M S に、起動処理 < A - 2 > 、通信処理 < A - 3 > 、会員登録依頼処理（ < A - 4 - 2 > ） 、メニュー登録依頼処理（ < A - 5 - 2 > ） 、認証代行依頼処理（ < A - 6 - 2 > ）を含む処理を実行させる。各処理については後述する。

ROM 6 3 は、CPU 6 2 が上記の各処理を実行するソフトウェア、CPU 6 2 が参照する各種データならびにその他のソフトウェアおよび情報を記憶する。特に、インターネット上のWWW (World Wide Web) サービスを携帯電話機MSから利用できるようにするためのブラウザ (browser) ソフトウェア、および最初にブラウザがアクセスするURI (ホームURI と称す。) 5 として、ゲートウェイサーバGWS上のUI情報が格納されているリソースを指定するURIが記憶されている。

本実施例におけるブラウザは、全体認証情報の入力タグを含むHTMLデータを取得すると、当該入力タグを識別することができる。さらに、当該ブラウザは、入力タグが指定する全体認証情報の入力を携帯電話機の使用者に促す画面を表示して、当該使用者により全体認証情報が入力されると、当該HTMLデータの取得先に、入力された全体認証情報を送信することができる。本実施形態において全体認証情報の入力タグが指定する処理は、「音声信号の取得」と音声信号および指紋画像の取得」を含む。

15 フラッシュメモリ (不揮発性メモリ) 6 4 は、CPU 6 2 から渡されたデータを記憶する

RAM 6 5 は、CPU 6 2 のワークメモリとして使用される。

(決定ボタン41)

20 図6は、本実施形態における携帯電話MS1の操作部4に設けられる決定ボタン41の内部構造を示す概略図である。

同図に示すように、決定ボタン41の内部には、透過板411、透過板411を保持する支持部材412、携帯電話機筐体に固定して設けられた支持部材413、支持部材413に取り付けられたカメラ42、光源43、および透過板411、支持部材412、支持部材413、カメラ42、光源43 25 で画定される内部空隙が設けられている。

透過板411および支持部材412は、図中上方から使用者の指によって押されると、図中下方に動き、押圧力が弱められると元の位置に戻るよう構成されている。透過板411には、ガラスやアクリルを含む、透明素材あ

るいは半透明素材を使用することができる。

カメラ 4 2 は、透過板 4 1 1 を介して透過板 4 1 1 を押圧する指の腹（指紋）を撮像するように配置されている。カメラ 4 2 には、C C D

（Charge-Coupled Devices）カメラを使用することができる。

- 5 光源 4 3 は、使用者の押圧する指が均等に照らし出されるように、カメラ 4 2 の周囲に環状に配置されている。光源 4 3 には、L E D（Light Emitting Diode）を使用することができる。

< A - 2 . 起動処理 >

- 10 認証代行装置 P V C の C P U 5 2 は、電源投入時に、R O M 5 3 に記憶されたソフトウェアを実行し、認証代行装置 P V C に、S S L 通信、会員登録処理、メニュー登録処理、認証代行処理およびサイト登録処理の受付を開始させる。また、C P U 5 2 は、認証代行装置 P V C に、保険・課金処理を開始させる。

- 15 携帯電話機 M S の C P U 6 2 は、電源投入時に、R O M 5 3 に記憶されたソフトウェアを実行した後、操作部 4 から入力される指示を監視する。C P U 6 2 は、W W W サービスの利用開始を示す指示を検知すると、R O M 6 3 に記憶されたブラウザを実行する。C P U 6 2 は、無線通信部を制御して、携帯電話機 M S を移動通信網に接続させる。

- 20 ブラウザは、ゲートウェイサーバ G W S に、R O M 6 2 に記憶されているホーム U R I が指定するゲートウェイサーバ内に記憶されている U I 情報に対する G E T 要求を送信する。

C P U 6 2 は、U I 情報を受信すると、当該 U I 情報に基づいて、ユーザインタフェースを携帯電話機 M S の使用者に提供し、起動処理が完了する。

- 25 この時、携帯電話機 M S の表示部 5 にはメインメニュー（例えば、図 7 の画面 G 1 1 1）が表示されている。

< A - 3 . 通信処理 >

携帯電話機 M S で動作するブラウザが、S S L 通信要求を認証代行装置 P

V Cに送信する。

認証代行装置P V Cは、S S L通信の開始要求を受信すると、S S Lハンドシェイクプロトコルにしたがって、当該携帯電話機M Sとハンドシェイクを開始する。

- 5 認証代行装置P V Cは、当該携帯電話機M Sとの間のセッションが新規に確立すると、S S L通信を開始する。認証代行装置P V Cは、当該セッションが確立されない場合は、S S L通信を行わないで通信を終了する。このように、S S L通信を利用することにより、送受信される情報（特に音声や指紋画像を含む情報）が第3者に悪用される危険性を小さくすることができる。

- 10 携帯電話機M Sは、サイトS 1との間においてS S L通信をおこなう。

認証代行装置P V Cは、サイトS 1との間においてS S L通信をおこなうことができる。

< A - 4 . 会員登録処理 >

- 15 < A - 4 - 1 . 概要 >

- 図8は、本実施例における認証サービスを利用希望する者が、自己の所有する携帯電話機M S 2から、本実施例における認証サービスに会員登録する場合の流れを示す図である。当該利用者および携帯電話機M S 2の電話番号および携帯電話M S 2の使用者の呼称（ここでは“B”）は、個人データベースT 1に記憶されていないものとする。

（ステップ101）：携帯電話機M S 2と認証代行装置P V Cの間でS S L通信を開始する。

- （ステップ102）：携帯電話機M S 2は、S S L通信が開始すると、認証代行装置P V Cに、携帯電話機M S 2の電話番号情報を含むG E T要求信号を送信する。

（ステップ103）：認証代行装置P V Cは、G E T要求信号を受信すると、携帯電話機M S 2の使用者が、認証サービスの会員であるかどうかを判定する。

認証サービスの会員でないことを検知すると、携帯電話機M S 2に、認証

レベル選択要求を含む信号を送信する。

認証サービスの会員であるときは、認証代行処理に進む。認証代行処理については後述する。

5 (ステップ104) : 携帯電話機MS2は、認証レベル選択要求を含む信号を受信すると、使用者に認証レベルを選択する画面を表示する。

携帯電話機MS2は、使用者により認証レベルの選択が行われると、選択された認証レベル情報を、認証代行装置PVCに送信する。

(ステップ105) : 認証代行装置PVCは、携帯電話機MS2に、基準情報入力フォームを含む信号を送信する。

10 (ステップ106) : 携帯電話機MS2は、基準情報入力フォームを含む情報を受信すると、携帯電話機MS2の使用者に前提認証情報の入力を促す。

携帯電話機MS2は、使用者による全体認証情報が入力されると、入力された全体認証情報を、認証代行装置PVCに送信する。

15 (ステップ107) : 認証代行装置PVCは、受信した全体認証情報の登録を終了し、会員登録を完了する。

本実施形態では、会員登録完了直後には全体認証を省略することができるので、認証代行装置PVCは、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機MS2に送信する。パスポートメニュー信号については後述する。

20

< A-4-2. 端末装置における会員登録依頼処理動作 >

(ステップ101) : 携帯電話機MS2は、使用者により、メインメニュー(図7の画面G111)から「パスポート」が選択されると、認証代行装置PVCとの間でSSL通信を開始する。

25 (ステップ102) : 携帯電話機MS2は、認証代行装置PVCに、携帯電話機MS2の電話番号を含むGET要求を送信する。

(ステップ103) : 携帯電話機MS2は、認証レベル選択要求を含む信号を受信すると、当該認証レベル選択要求に基づいて、認証レベルの選択を促す画面(例えば図7の画面G131)を表示部5に表示する。

(ステップ104) : 携帯電話機MS2は、使用者によって、「音声のみ」が選択されると、「音声のみ」に対応した情報を含む認証レベル（本実施形態では「音声のみ」の場合に“1”と、「指紋情報および声紋情報」の場合に“3”とする。）を、認証代行装置PVCに送信する。

- 5 (ステップ105) : 携帯電話機MS2は、基準情報入力フォームを受信すると、基準情報入力フォームに含まれる全体認証情報入力のタグを解釈する。先に選択した認証レベルが「音声のみ」を示す“1”であることから、携帯電話機MS2は、当該入力フォームに音声入力のタグを検知して、これを解釈し、音声の入力を促す画面（例えば図7の画面G132）を表示部5に表示する。（図9のステップSA1、2）

(ステップ106) : 携帯電話機MS2は、決定ボタン41の使用者による押下げを検知すると、押下げ時点で音響入力部3から入力している音声を、全体認証情報として、認証代行装置PVCに送信し、会員登録以来処理を完了する。

15

< A - 4 - 3. 認証代行装置における会員登録処理動作 >

(ステップ101) : 認証代行装置PVCと携帯電話機MS2の間でSSL通信を開始する。

- 20 (ステップ102) : 認証代行装置PVCは、通信部P1を介して、非会員から送信されたGET要求を受信する。

(ステップ103) : 認証代行装置PVCは、受信したGET要求に含まれる携帯電話MS2の電話番号をキーとして、個人用テーブルT1を検索する。

- 25 認証代行装置PVCは、当該電話番号を含むレコードが個人用テーブルT1に登録されていないことを検知すると、当該テーブルT1にレコードを追加する。

認証代行装置PVCは、当該追加したレコードの会員番号フィールドに、重複しない会員番号を生成して格納し、当該レコードの使用料フィールドに使用料“100”を格納する。

認証代行装置PVCは、認証レベル選択要求を含む信号を、携帯電話機M

S 2 に送信する。

(ステップ 1 0 4) : 認証代行装置 P V C は、受信した「音声のみ」を示す認証レベル” 1 ”を、当該レコードの認証レベルフィールドに格納する。

5 (ステップ 1 0 5) : 認証代行装置 P V C は、「音声のみ」を示す認証レベル” 1 ”に対応して、全体認証情報として音声の入力タグおよび利用者の呼称の入力タグを含んだ基準情報入力フォームを含む信号を、携帯電話機 M S 2 に送信する。

10 認証代行装置 P V C は、当該認証レベル「音声のみ」を示す認証レベル” 1 ”に応じた値 “ 1 0 0 ” (認証レベルが “ 2 ” の場合には “ 5 0 ” 、 “ 3 ” の場合には “ 0 ”) を当該レコードの保険料フィールドに格納する。

(ステップ 1 0 6) : 認証代行装置 P V C は、全体認証情報として音声を受信する。

認証代行装置 P V C は、受信した音声から声紋情報を生成して、この声紋情報を当該レコードの声紋情報フィールドに暗号化して格納する。

15 また、認証代行装置 P V C は、使用者の呼称を含んだ情報を受信すると、受信した呼称を当該レコードの名前フィールドに登録する。

さらに、認証代行装置 P V C は、現在時刻を取得して、現在時刻よりもある時間先となる時刻を有効期限として、当該レコードの有効期限フィールドに格納する。

20 有効期限の設定は、利用者がおこなえるようにできる。例えば、基準情報入力フォームに有効期限の入力タグを設けることによって実現できる。

また、個人テーブル T 1 にシフト時間フィールドを追加し、基準情報入力フォームにシフト時間の入力タグを設けることによって、有効期限をシフト時間という有効時間で決定することも可能である。

25 (ステップ 1 0 7) : 認証代行装置 P V C は、(ステップ 1 0 6) の処理が終了すると、会員登録処理を完了する。

認証代行装置 P V C は、携帯電話機 M S 2 にパスポートメニュー信号を含む信号を送信し、会員登録処理が完了する。本実施形態では、会員登録完了直後には全体認証を省略することができるので、認証代行装置 P V C は、認

証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機MS 2に送信する。

<A-5. メニュー登録処理>

5 <A-5-1. 概要>

図10は、本実施例における認証代行サービスの会員が、自己の所有する携帯電話機MS 2から、認証代行装置PVCの提供する認証サービスにメニュー登録する場合の処理の流れを示す図である。携帯電話機MS 2は全体認証が完了しているものとする。

- 10 ここで、携帯電話機MS 2の電話番号および携帯電話機MS 2の使用者の呼称（ここでは“B”）は、個人用テーブルT1に登録されているものとする。

（ステップ201）：携帯電話機MS 2は、メニュー登録処理に移ることを示す選択情報を含む信号を、認証代行装置PVCに送信する。

- 15 （ステップ202）：認証代行装置PVCは、当該選択情報を含む信号を受信すると、複数のサイトの接続先IDを含む登録選択メニューを含む信号を、携帯電話機MS 2に送信する。

- 20 （ステップ203）：携帯電話機MS 2は、当該登録選択メニューを含む信号を受信すると、サイトの選択を利用者に促す画面を表示する（例えば、図6の画面G134）。

携帯電話機MS 2は、サイトが選択されると、選択されたサイトの接続先IDを含む信号を、認証代行装置PVCに送信する。

（ステップ204）：認証代行装置PVCは、接続先IDを含む信号を受信すると、個別登録フォームを含む信号を、携帯電話MS 2に送信する。

- 25 （ステップ205）：携帯電話機MS 2は、個別登録フォームを含む信号を受信すると、個別登録フォームに基づいて、当該サイトに対応した個別認証情報の入力を促す画面を表示する（例えば、図7のG135）。

携帯電話機MS 2は、個別認証情報が入力されると、当該個別認証情報を含む信号を、認証代行装置PVCに送信する。

(ステップ206) : 認証代行装置PVCは、個別認証情報を含む信号を受信すると、メニュー登録を行う。

認証代行装置PVCは、登録完了通知を含む信号を、携帯電話機MS2に送信する。

- 5 (ステップ207) : 携帯電話機MS2は、登録完了通知を含む信号を受信すると、確認通知を含む信号を、認証代行装置PVCに送信する。

- (ステップ208) : 認証代行装置PVCは、確認通知を含む信号を受信すると、メニュー登録処理を完了する。本実施形態では、メニュー登録完了直後には全体認証を省略することができるので、認証代行装置PVCは、認証
10 サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機MS2に送信する。

< A-5-2. 携帯電話機MSのメニュー登録依頼時の動作 >

- (ステップ201) 携帯電話機MS2は、パスポートメニュー信号から「新規登録」が利用者により選択されると、「新規登録」を選択したことを示す
15 選択情報を含む信号を、認証代行装置PVCに送信する。

(ステップ202) 携帯電話機MS2は、当該登録選択メニューを受信すると、認証代行の対象の登録を促す画面（例えば図7の画面G134）を表示部5に表示する。

- 20 (ステップ203) 携帯電話機MS2は、使用者によって所望の対象（ここでは“懸賞クイズ”）が選択されると、この選択に対応した接続先ID（ここでは“5”）を、認証代行装置PVCに送信する。

- (ステップ204) 携帯電話機MS2は、個別認証登録フォームを受信すると、個別認証登録フォームに基づいて、IDのみの入力を促す画面（例えば
25 図7の画面G135）を、表示部5に表示する。

(ステップ205) 携帯電話機MS2は、ID（ここでは“65883”）が使用者により入力され、送信ボタンの使用者による押下を検知すると、入力されたIDを、個別認証情報として認証代行装置PVCに送信する。

(ステップ206) 携帯電話機MS2は、登録完了通知（あるいは書式違反

通知)を受信すると、接続先の新規登録が完了(あるいは失敗)した旨を使用者に通知する画面(例えば図7の画面G136あるいは画面G137)を表示部5に表示する。

- (ステップ207) 携帯電話機MS2は、登録完了通知の画面あるいは書式違反通知の画面の“次へ”ボタンの使用者による押下げを検知すると、確認通知を認証代行装置PVCに送信し、メニュー登録依頼処理を成功(あるいは失敗)して終了する。

< A-5-3. 認証代行装置PVCのメニュー登録処理時の動作 >

- 10 (ステップ202) 認証代行装置PVCは、選択情報を含む信号を受信すると、認証代行の対象を選択するための登録選択メニューを、携帯電話機MS2に送信する。

この登録選択メニューは、選択可能な全ての接続先の接続先IDおよびタイトルを含んでいる。(図11のステップSB14)

- 15 (ステップ204) 認証代行装置PVCは、接続先IDを受信すると、当該接続先IDで特定されるレコードを、サイト別テーブルT2から抽出する。

認証代行装置PVCは、当該レコードのID要否およびパスワード要否フィールドの内容(ここではIDを要するが、パスワードは不要)に対応した個別認証登録フォームを、携帯電話機MS2に送信する。(図11のステップSB15)

(ステップ206) 認証代行装置PVCは、IDを受信すると、入力されたIDが、サイト別テーブルT2の当該レコードのID属性フィールドに記憶されたID属性(ここでは、4バイト以上8バイト以下であること)の条件に適合するか判定する。(図11のステップSB16)

- 25 認証代行装置PVCは、当該IDがID属性を適合すると、個人用テーブルT1の該当するレコード(会員番号が“2”のレコード)の接続先IDおよびIDのフィールドに“5”および“65883”の組を追記する。

認証代行装置PVCは、登録完了通知を携帯電話機MS2に送信する。(図11のステップSB17)

認証代行装置PVCは、当該IDがID属性に適合しない場合、書式違反通知を、携帯電話機MS2に送信する（図11のステップSB18）。

（ステップ208）：認証代行装置PVCは、確認通知を含む信号を受信すると、メニュー登録処理を完了する（図11のステップSB19）。本実施形態では、メニュー登録完了直後には全体認証を省略することができるので、
5 認証代行装置PVCは、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機MS2に送信する。

<A-6. 認証代行処理（パスポートメニュー）>

10 <A-6-1. 概要>

図12は、本実施例の認証サービスの会員が自己の所有する携帯電話機MS1から、認証代行装置PVCの提供する認証サービスを利用して、サイトS1が提供する会員制サービスを利用する場合の処理の流れを示す図である。

ここで、携帯電話機MS1の電話番号および携帯電話機MS1の使用者の
15 呼称（ここでは“C”）は、個人用テーブルT1に登録されているものとする。

また、当該会員は、会員登録時に認証レベルに「音声＋指紋」を選択しているとする。

さらに、当該会員が携帯電話機MS1から最後に認証サービスを利用して
20 から数時間以上経過しているものとする。

（ステップ301）認証代行装置PVCと携帯電話機MS1の間でSSL通信が開始する。

（ステップ302）携帯電話機MS1は、SSL通信セッションが確立すると、認証代行装置PVCに、携帯電話機MS1の電話番号を含むGET要求
25 信号を送信する。

（ステップ303）認証代行装置PVCは、GET要求信号を受信すると認証情報入力フォーム情報を含む信号を、携帯電話機MS3に送信する。

（ステップ304）携帯電話機MS1は、認証情報入力フォーム情報を含む信号を受信すると、携帯電話機MS1の使用者に全体認証情報の入力を促す。

携帯電話機MS 1は、使用者により全体認証情報が入力されると、入力された全体認証情報を、認証代行装置PVCに送信する。

(ステップ305) : 認証代行装置PVCは、全体認証情報を受信すると、認証処理をおこなう。

- 5 認証代行装置PVCは、認証処理に成功すると、認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機MS 1に送信する。

認証代行装置PVCは、認証処理に失敗すると、認証失敗通知を、携帯電話機MS 1に送信し、認証代行処理を失敗して完了する。

- 10 (ステップ306) 携帯電話機MS 1は、パスポートメニュー信号から、一つのサイトが使用者によって選択されたことを検出すると、当該サイトの情報を含む選択情報を、認証代行装置PVCに送信する。

(ステップ307) 認証代行装置PVCは、選択情報を受信すると、個別ログイン情報を生成して、当該個別ログイン情報を、携帯電話機MS 1に送信する。

- 15 (ステップ308) 携帯電話機MS 1は、個別ログイン情報を受信すると、当該個別ログイン情報に記載されている方法で、サイトS 1との間でSSL通信を開始する。

(ステップ309) : 携帯電話機MS 1は、SSL通信が開始すると、当該個別ログイン情報に記載されている方法で、サイトS 1にログインする。

- 20 サイトS 1は、携帯電話機MS 1の使用者のログインについて、会員情報データベースCDB 1を参照して認証処理を行う。

(ステップ310) サイトS 1は、当該使用者の認証に成功すると、利用者にコンテンツの提供を含む会員制サービスの提供をおこなう。

サイトS 1は、当該使用者の認証に失敗すると、認証処理を終了する。

25

< A - 6 - 2 . 携帯電話MSにおける認証代行依頼処理の動作 >

(ステップ301) 携帯電話機MS 1は、メインメニュー (図7の画面G 111) から「パスポート」を携帯電話機MS 1の使用者により選択されたことを検知すると、認証代行装置PVCとの間でSSL通信を開始する。

(ステップ302) : 携帯電話機MS1は、認証代行装置PVCに、携帯電話機MS1の電話番号を含むGET要求を送信する。

(ステップ303) 携帯電話機MS1のCPU62は、「音声信号および指紋画像の取得」を指定するタグを含む全体認証情報入力フォームを受信すると、当該入力タグに基づいて、全体認証情報の入力を促す画面（例えば図15の画面G112）を表示部5に表示する。

(ステップ304) CPU62は、決定ボタン41の使用者による押下げを検知すると、LED光源43を点灯して、CCDカメラ42に写る像を記録（撮像）する。

10 この時、CCDカメラ42は、決定ボタン41を押し下げている指の腹を、透過板411越しに撮像する。

CPU62は、決定ボタン41の使用者による押下げ時に、音響入力部3から入力していた音声を取得する。（図9のステップSA1、3）

CPU62は、撮像された指紋画像と音声を、全体認証情報として認証代行装置PVCに送信する。

(ステップ305) 携帯電話機MS1は、パスポートメニュー信号を受信すると、認証代行の対象の選択を促す画面（例えば図13の画面G151）を、表示部に表示する。

(ステップ306) 携帯電話機MS1は、サイト「D社ポイント」が使用者によって選択されたことを検知すると、このサイトを選択したことを示す選択情報を、認証代行装置PVCに送信する。

(ステップ308) 携帯電話機MS1は、個別ログイン情報を受信すると、当該個別ログイン情報に記述されているサイトS1とSSL通信を開始する。

(ステップ309) 携帯電話機MS1は、サイトS1とSSL通信が開始するのを待って、当該個別ログイン情報に記述されているGET要求のシーケンスを、個別ログイン情報に記述されているサイトS1で個別認証処理をおこなっているリソース“//www.c.co.jp/point/point.cgi”に送信する。この送信によって、手動でのログイン手続きの代行をおこなっている。

(ステップ310) サイトS1は、当該GET要求を受信すると、携帯電話

機MS 1の認証処理を開始する。IDとパスワードに“docom”と“*****”がそれぞれ正しく入力されているので、携帯電話機MS 1の使用者はサイトS 1の提供するサービスの会員であると認証される。

5 サイトS 1は、以降、当該使用者の個人用サービスコンテンツ（情報）を携帯電話機MS 1に送信する。（ここでは当該サイトS 1が提供するショッピングサービスの利用で取得した当該携帯電話機MS 1の累計ポイントを示す情報が送信されている。）

10 携帯電話機MS 1は、当該コンテンツを受信すると、使用者が取得したポイントを通知する画面（例えば図7の画面G 1 5 2）を、表示部5に表示する。

< A - 6 - 3 . 認証代行装置PVCの認証代行処理時の動作 >

（ステップ301）認証代行装置PVCと携帯電話機MS 1はSSL通信を開始する。（図11のステップSB1）

15 （ステップ302）認証代行装置PVCは、携帯電話機の電話番号を含むGET要求信号を受信すると、個人用テーブルT1参照して、当該電話番号を含むレコードを検索する。認証代行装置PVCは、検索に成功すると、当該レコードを抽出する。ここでは、会員番号フィールドに“1”が格納されたレコードが抽出される。（図11のステップSB2）

20 認証代行装置PVCは、現在時刻を取得して、当該レコードの有効期限フィールドと時刻の比較をおこなう。ここでは、最後に認証サービスを受けてから長時間経過しているため、全体認証は有効期限切れである。（図11のステップSB4）

25 （ステップ303）認証代行装置PVCは、当該レコードの認証レベルが“2”であるから、「音声信号および指紋画像の取得」を指定する入力タグを含む認証情報入力フォームを、携帯電話機MS 1に送信する。（図11のステップSB5）。

（ステップ304） 認証代行装置PVCは、全体認証情報として音声および指紋画像を受信する。（図11のステップSB5）

認証代行装置 P V C は、これらの音声および指紋画像から声紋情報および指紋情報を生成する。

5 認証代行装置 P V C は、当該声紋情報および指紋情報と、先に選択したレコードに格納されている全体認証基準情報（ここでは声紋基準情報および指紋基準情報）と照合する。

この時、認証代行装置 P V C は、当該レコードに暗号化されて記憶されていた全体認証基準情報を読み出す時に暗号解読して、照合に使用して、照合完了後に破棄する。このようにして、基準情報の漏洩を防止している。（図 1 1 のステップ S B 6）

10 図 1 4 は、認証代行装置における認証処理過程の流れを示す図である。同図に示すように、認証処理過程は、フィルタ処理、周波数分析処理、特徴抽出処理、特徴正規化処理、照合を含む。

（フィルタ処理）：認証代行装置 P V C は、受信した生体固有情報（ここでは、指紋画像あるいは音声）を含んだ生データから有用な情報を含む帯域以外
15 外の信号を除去する。

（周波数分析処理）：認証代行装置 P V C は、フィルタにかけられたデータについて、空間あるいは時間周波数分析処理を行う。

（特徴抽出処理）：認証代行装置 P V C は、周波数分析処理された信号から対象となる生体情報を特徴付ける特徴パラメータを抽出する。

20 （特徴正規化処理）：認証代行装置 P V C は、得られた個々の特徴パラメータを正規化して、正規化特徴パラメータを得る。

（照合）：認証代行装置 P V C は、前記正規化特徴パラメータと全体認証基準情報を照合する。本実施形態における照合の方法は、パターンマッチング法を含む方法を採用することができる。

25 認証代行装置 P V C は、照合に成功すると、現在時刻からある時間（例えば 3 0 分）経過させた時刻を当該レコードの有効期限フィールドに格納する。

（図 1 1 のステップ S B 8）

（ステップ 3 0 5）認証代行装置 P V C は、個人テーブル T 1 を参照して、認証に成功した携帯電話機の使用者のレコードを参照して、当該使用者が、

登録してある複数の接続先 I D を抽出し、抽出した接続先 I D をキーとして、サイトテーブル T 2 を参照して、接続先 I D に対応したレコードから、サイトのタイトルおよび分類を抽出する。

5 認証代行装置 P V C は、抽出した接続先のタイトル名と接続先 I D 情報を含むパスポートメニュー信号を生成する。ここでは、接続先 I D が “ 7 ” の接続先に対応したタイトル「D社ポイント」および接続先 I D ” 7 ” ならびに、接続先 I D が “ 5 ” の接続先に対応したタイトル「懸賞リスト」および接続先 I D ” 5 ” を含むパスポートメニュー信号を生成する。

10 本実施例では、さらに、パスポートメニュー信号に、「新規登録」というタイトルの接続情報が認証代行装置 P V C によって付け加えられている。

認証代行装置 P V C は、このように生成された認証サービスの対象を選択するためのパスポートメニュー信号を、携帯電話機 M S 1 に送信する（図 1 1 のステップ S B 9）。

15 （ステップ 3 0 6）認証代行装置 P V C は、選択情報を受信すると、当該選択情報の種別を判定する。認証代行装置 P V C は、当該選択情報が新規メニュー登録を要求する場合には、メニュー登録処理に移行する（図 1 0 ステップ S B 1 2）。ここでは、接続先 I D “ 7 ” が選ばれたとする。

20 （ステップ 3 0 7）認証代行装置 P V C は、当該選択情報に含まれる接続先 I D をキーとして、テーブル T 1 および T 2 を参照して、個別ログイン情報を生成する。

この個別ログイン情報は、その解釈・実行時に G E T 要求を自動的に送出するように記述された H T M L データであり、当該接続先 I D に対応した接続先のへ個別認証情報を渡す旨のシーケンスが当該 G E T 要求に含まれるように記述されている。ここでは、接続先 I D “ 7 ”、タイトル「D社ポイント」であるサイトが要求する個別ログイン情報と会員番号 “ 1 ” から、個別
25 ログイン情報が生成される。

認証代行装置 P V C は、当該個別ログイン情報を携帯電話機 M S 1 に送信し、認証代行処理を完了する（図 1 1 のステップ S B 1 3）。

< A - 6 B . 全体認証情報入力の有効期限と全体認証入力省略場面 >

図 1 0 に示す認証代行装置のフローチャートには、全体認証入力省略されて個別認証代行処理が行われる 2 つのケースが示されている。

第 1 のケースでは、認証代行装置 P V C は、会員登録（ステップ S B 3）を完了すると、（ステップ S B 2）から（ステップ S B 4）の処理に進む。このケースでは、有効期限が、会員登録時に会員登録時点より経過した時刻として設定されたばかりであるから、その時点は全体認証の有効期限内にあると判定される。したがって、認証代行装置 P V C は、全体認証処理を省略して、パスポートメニュー（ステップ S B 9）に進むことができる。このように、会員登録後に利用者にパスポートメニューを使用することを許可している。この間、携帯電話の画面は、例えば、図 7 の画面 G 1 3 2 - G 1 3 8 - G 1 3 9 のように変化する。

第 2 のケースでは、認証代行装置 P V C は、メニュー登録が完了する（ステップ S B 1 9）と、（ステップ S B 4）に進む。この時点で、全体認証が有効期限内となるように、有効期限を設定しておくことによって、利用者は、メニュー登録でパスポートメニューに新規に追加したサイトを選んで認証サービスを受けることができる。ただし、サイト登録中に全体認証情報入力の有効期間を経過した場合には、全体認証情報入力を再度しなければならない。

第 3 のケースは、図 1 5 に示す本実施形態における認証サービスの会員が、自己の所有する携帯電話機 M S 1 を使用して、サイト S 1 を利用した後に、サイト S 2 を利用する場合である。この間、携帯電話の画面は、例えば、図 1 3 の画面 G 1 5 1 - G 1 5 2 - G 1 5 1 - G 1 5 3 のように変化する。ただし、サイト S 1 利用中に全体認証情報入力の有効期間を経過した場合には、サイト S 2 を利用する時に、全体認証情報入力を再度しなければならない。

このようにして、認証代行装置 P V C は、全体認証情報入力の有効期限を管理することによって、利用者の利便性とセキュリティのバランスを保っている。

< C - 6 C . 認証サービスの不正利用時 >

ここでは、認証代行サービスの正当な会員（会員番号は“3”）が所有する携帯電話機MS3を拾った第3者（以後、使用者）が認証代行サービスを受けようとした場合を想定している。なお、使用者が携帯電話機MS3を拾ったのは、正当な会員が最後に認証代行サービスを利用してから数時間経過した時点とする。

この場合、図16に示すように、使用者が携帯電話機MS3を操作し、メインメニュー（図17の画面G111）から「パスポート」を選択すると、携帯電話機MS3から認証代行装置PVCへ接続要求が送信され、両者の間でSSLのハンドシェークが行われ、両者間でSSL通信が可能となる（図11のステップSB1）。

次に、携帯電話機MS3から認証代行装置PVCへ、「パスポート」の選択に応じたGET要求が送信される。このGET要求を受信した認証代行装置PVCでは、当該GET要求に含まれている電話番号をキーとして個人用テーブルT1が検索され（図11のステップSB2）、結果として、会員番号フィールドに“3”が格納されたレコードが抽出される。このレコードの有効期限フィールドには現在時刻以前の時刻が格納されていることから、このレコードに基づいた認証情報入力フォームが、GET要求の応答として認証代行装置PVCから携帯電話機MS3へ送信される（図11のステップSB4、SB5）。なお、会員番号フィールドに“3”が格納されたレコードの認証レベルフィールドには“1”が格納されていることから、認証情報入力フォーム中の入力タグは、「音声信号の取得」を指定するタグとなる。

この認証情報入力フォームを受信した携帯電話機MS3では、当該認証情報入力フォームが解釈・実行され、全体認証情報の入力を促す画面（例えば図の画面G112）が表示される。この画面を視認した使用者が発音しながら決定ボタン41を押すと、その時点で音響入力部3から入力されている音声信号が、全体認証情報として認証代行装置PVCへ送信される。

全体認証情報として音声信号を受信した認証代行装置PVCでは、この音声信号から声紋情報が生成され、この声紋情報と、先に選択したレコードに格納されている声紋情報とが照合される（図11のステップSB5、SB6）。

後者の声紋情報は正当な会員の声紋情報であることから、両者が一致することはない。よって、認証代行装置PVCでは認証に失敗したと判断され、携帯電話機MS3から認証代行装置PVCへ認証失敗通知が送信される（図1のステップSB7, SB10）。この結果、携帯電話機MS3には、全体
5 認証に失敗した旨を示す画面（例えば図17の画面G112）が表示される。

< A-7. 保険、課金処理 >

本実施例の認証システムは、利用者が会員登録時に、選択した全体認証に利用する認証レベルに基づいて保険料が定められる。本実施例では、認証レ
10 ベルとして1から3が提供され、図18に示すように、それぞれ利用する照合情報と保険料が設定されている。

認証代行装置PVCは、利用者が選択した認証レベルを個人データベースT1の認証レベルフィールドに格納し、保険料フィールドに当該認証レベルに対応する保険料を格納する。

15 認証代行装置PVCは、ある時点で、個人用テーブルT1の当該フィールドに格納されている保険料と使用料を合計した金額を、端末装置の複数の使用者に、それぞれ請求する。

認証代行装置PVCは、この時、上記金額と端末装置の電話番号を含む請求情報を生成して、これを移動通信網MPNへ送信することによって、移動
20 通信網MPNに課金処理を依頼しても良い。

移動通信網MPNは、この請求に通信料を加えた金額を、端末装置の使用者に請求する。

< A-8. サイト登録処理 >

25 本実施形態の認証システムは、認証代行装置PVCのサイト別テーブルT2にレコードを追加する機能を有する。

認証システム代行装置PVCは、エージェントプログラムを実行することによって、インターネットに接続された会員制サービスを提供しているサイトの情報を収集し、当該サイトそれぞれについて、自動的にサイト別テーブ

ルT 2にレコードを追加して、サイト登録を行うようにしてもよい。

このエージェントプログラムは、会員がIDやパスワードをサイト毎に記述された認証プログラムに渡す旨のシーケンスが記述されたHTMLデータを、インターネット上で収集する。このエージェントプログラムは、収集したHTMLデータを解析して、当該HTMLデータに記述されているID入力やパスワード入力を示すタグを検出して、当該IDやパスワードに要求される属性（使用できる文字数、使用できる文字種を含む情報）を判別して、サイト別データベースT 2のID属性およびパスワード属性フィールドに格納する。

さらに、このエージェントプログラムは、収集したHTMLデータを得たサイトに含まれるタグで指定された情報に基づいて、当該サイトの分類を試み、サイト別データベースT 2の当該サイトに対応するレコードの分類フィールドに、得られた分類名を格納するようにしてもよい。

また、本実施形態の認証代行装置PVCは、外部（例えばサイトS 1の運営者）の指示に従い、サイト別テーブルT 2の任意のレコード内の接続情報、分類、ID可否、パスワード可否、ID属性、およびパスワード属性のフィールドの内容を変更する機能を有する。

< B. 第2実施形態 >

本発明の第2の実施形態における認証システムの構成は、図1のブロック図に示す第1の実施形態と同一構成をとる。

< B-1. 認証代行処理 >

図19は、本実施例における認証サービスをの会員が、自己の所有する携帯電話機MS 3から、認証代行装置PVCの提供する認証サービスを利用して、サイトS 1が提供する会員制サービスを利用する場合の処理の流れを示す図である。

ここで、認証サービスを利用する携帯電話機MS 3の使用者は、会員登録時に、認証レベル”1”「声紋情報を使用する」ことを選択してあるとする。

また、認証代行サービスの利用者は、充分長い時間、認証代行サービスを

利用していなかったとする。

図 1 9 に示される処理と、図 1 2 に示される第 1 の実施例における認証処理は共通部分が多いので、異なる部分についてのみ説明を加える。

5 (ステップ 4 0 3) 携帯電話機 M S 3 の C P U 6 2 は、「音声信号の取得」を指定するタグを含む全体認証情報入力フォームを受信すると、当該入力タグに基づいて、全体認証情報の入力を促す画面（例えば図 1 3 の画面 G 1 1 2）を表示部 5 に表示する。

(ステップ 4 0 4) C P U 6 2 は、決定ボタン 4 1 の使用者による押下げ時に、音響入力部 3 から入力していた音声を取得する。

10 C P U 6 2 は、取得した音声について、認証処理前段処理を行う。

本実施例において認証処理前段処理はフィルタ処理、周波数処理、特徴抽出処理および特徴正規化処理を含む。

携帯電話機 M S 1 は、当該前段処理が行われると、正規化特徴情報を、認証代行装置 P V C に送信する。

15 (ステップ 4 0 5) 認証代行装置 P V C は、正規化特徴情報を受信すると、認証処理後段処理として、受信した正規化特徴情報と、個人テーブル T 1 の該当するテーブルに記憶されている全体認証基準情報とを照合する。

認証代行装置 P V C は、照合に成功すると、携帯電話機 M S 3 に、パスワードメニュー信号を送信する。

20

< C . 変形例 >

< C - 1 . 変形例 1 > 本実施形態の認証システムは、携帯電話機 M S に固定されている電話番号をキーとして個人用テーブル T 1 を検索して、全体認証処理をしているが、電話番号の代わりに携帯電話機 M S の使用者の I D を
25 キーとして個人用テーブル T 1 を検索して、全体認証処理をしてもよい。さらに電話機使用者の生体情報をキーとして個人用テーブル T 1 を検索して、全体認証処理をしてもよい。この場合、本実施例の認証サービスの利用者は、他人の携帯電話機 M S を借用して、当該サービスを利用することができるようになる。

＜C－2．変形例2＞ 本実施形態の認証システムは、声紋情報の照合を全体認証において必ず実行しているが、認証システムは声紋情報の照合を実行しないで、指紋情報の照合を実行するようにしてもよい。この場合、認証代行装置は個人用テーブル1の該当する使用者のレコードの認証レベルフィールドに、例えば、認証レベル“2”を書き込む。また、認証代行装置PVCは当該レコードの保険料フィールドに、保険料“50”を書き込む。

＜C－3．変形例3＞ 本実施例の認証システムは、虹彩パターン、
を含む生体固有情報を含む全体認証情報を利用してもよい。さらに、本実施例の認証システムは、生体情報でない高いセキュリティを確保できる情報を含む全体認証情報を利用してもよい。

＜C－4．変形例4＞ 本実施形態の認証システムは、携帯端末の契約者以外が使用することが可能なようにしても良い。例えば契約者本人が怪我をして、全体認証情報を入力できなくなった場合に、代理人が認証代行サービスを利用できるように、個人用テーブルT1の当該契約者のレコードに代理人用フィールドを追加して、当該フィールドに代理人の声紋情報（および指紋情報）を格納してもよい。この時、代理人が声紋情報（および指紋情報）を格納する方法は任意である。

＜C－5．変形例5＞ 本実施形態の認証代行装置PVCは、ゲートウェイサーバGWSを兼ねていてもよい。この場合は、認証代行装置PVCは、ゲートウェイサーバGWSが認証する携帯電話機MSの発（コーラー）IDを端末装置に固定された情報として利用して全体認証処理をおこなうことができる。さらにこの場合、セキュリティを確保できるならば、移動通信網MPN内にある携帯電話機と認証代行装置PVC（＝ゲートウェイサーバGWS）間では非暗号化通信をおこない、ゲートウェイサーバGWSとサイトS（S1－S2）間でのみ暗号化通信をおこなうようにしてもよい。すなわち、サ

サーバとサーバとの間でのみ暗号化通信を行うようにしてもよい。

- ＜C－6．変形例6＞ 本実施例の認証システムは、利用者がパスポートメニュー信号に登録されていないサイトを認証サービスの対象（すなわちパスポートメニュー信号）に追加登録することができるようにしてもよい。

携帯電話MSの利用者は、メニュー登録時に、パスポートメニュー信号に登録されていないサイトを追加する旨を指定して、追加希望サイトのタイトル、接続情報、分類、IDおよびパスワードの要否、個人認証情報（ID、パスワード）を手動で入力する。

- 10 認証代行装置PVCは、追加希望サイトの情報を受信すると、個人テーブルT1の当該利用者のレコードに当該追加サイトの情報を格納する。この時、認証代行装置PVCは、サイト別テーブルT2を参照して、重複しない接続先IDを付与する。

- 15 認証代行装置PVCは、個人テーブルT1にサイトの接続情報を格納する新たなフィールドを追加することによって、当該サイトの追加をおこなっても良い。

- あるいは、認証代行装置PVCは、サイト別テーブルT2にレコードを追加して、受信した追加サイトの情報を当該レコードに格納することによって、当該サイトの追加をおこなっても良い。さらに、認証代行装置PVCは、利用者にIDおよびパスワードの要否の入力を求めないで、受信した個人認証情報を解析してIDおよびパスワードの要否を判定するようにしても良い

- ＜C－7．変形例7＞ 本実施形態の端末装置は、ブラウザを搭載した携帯電話機に限定されない。本実施形態の端末装置は：固定電話機に接続して使用される、据え置き型コンピュータやブラウザを搭載したセットトップボックスを含むクッキー（Cookie）を取り扱うことができるクッキー対応端末装置；固定電話機に接続して使用される、PDA（Personal Data Assistant）や携帯ゲーム機器を含むクッキーを取り扱うことができないクッキー非対応端末装置；SIM（Subscriber Identity Module）やUIM（User Identity

Module) と組み合わせて使用する携帯電話機能を有するクッキー対応端末装置；携帯電話機に接続して使用されるクッキー対応端末装置；携帯電話機に接続して使用されるクッキー非対応端末装置；SIMやUIMと組み合わせて使用するクッキー非対応端末装置を含む。

- 5 本実施例におけるクッキーを使用することができる端末装置は、使用者を特定するIDをクッキーに記録して、このIDを端末装置に固定された情報として、全体認証処理で利用しても良い。

- 10 また、本実施例における携帯電話機（あるいはSIMやUIM）を使用する端末装置は、携帯電話機（あるいはSIMやUIM）に固定された電話番号を、端末装置に固定された情報として、全体認証処理で利用しても良い。

- 15 さらに、本実施例における携帯電話機は、クッキーを使用することができる携帯電話機も含む。この時、本実施例におけるクッキーを使用することができる携帯電話機は、使用者を特定するIDをクッキーに記録して、このIDを携帯電話機に固定された情報として、全体認証処理で利用しても良い。

< C - 8 . 変形例 8 >

本実施形態の端末装置は、指紋画像を入力する機能を備えていない携帯電話機MSを含むものとする。さらに、本実施形態の端末装置は、全体認証情報入力タグを判別することができない携帯電話機MSも含む。

- 20 本発明は上述した具体的な態様に限定されるものではなく、特許請求の範囲に記載された範囲内で任意の態様を含む。

< D . 補足 >

- 25 このように、本実施形態によれば、携帯電話機の利用者は、IDやパスワードの入力を要する、セキュリティの確保された各種の個人用サービスを利用する際に、個別の認証情報（IDやパスワード）を記憶しておく必要がない。さらに、個別認証情報は携帯電話機に記憶されないため、携帯電話機が第3者の手に渡っても、個別認証情報が漏洩する虞はない。

また、本実施形態によれば、第3者が認証代行サービスを不当に利用する

事態を確実に回避することができる。特に、全体認証情報として声紋情報や指紋情報等の生体情報を利用するようにしたことにより、パスワードや暗証番号を用いる場合に比較して、本人性の認証をより確実に行うことができる。さらに、生体情報は使用者による記憶を要さないため、使用者にかかる負担
5 が軽減されるという利点もある。

さらに、本実施形態によれば、指紋画像の取得機能を持たない携帯電話機MS 2を用いる使用者に対しても認証サービスを提供することができる。したがって、使用者は使用中の端末を買い換えることなくサービスを受けることができる。また、音声を入力する機能を備えた携帯電話機を用いたことにより、声紋認証のためのハードウェアを新設せずに済んでいる。
10

さらに、全体認証情報の入力および送信を指示するためのボタン内にCCDカメラを備え、全体認証情報の入力時にボタン上に存在する指を撮像して指紋画像を得るようにしたため、使用者は1回の操作で指紋画像の入力・送信を行うことができる。このことは、特に、ボタン操作を迅速に行うことが
15 困難な携帯電話機等の携帯端末において有利である。

また、全体認証に有効期限を設定し、有効期限内であれば全体認証を行わずとも認証代行サービスを受けられるようにしたことにより、使用者の手間を削減することができる。さらに、サイトから個別認証情報の入力を促すフォームが携帯電話機へ送信される前に、サイトにおいて個別認証情報を照合
20 する認証プログラムに対して個別認証情報が渡されるため、使用者は当該フォームの処理をスキップして所望のページを取得することができる。

また、認証レベルを選択可能としたことにより、多種のサービスを提供可能となり、使用者が所望のサービスを受けることができる可能性が高くなっている。例えば、認証の信頼度が低下しても古い携帯電話機を継続して使用
25 したい使用者や、信頼度が低くなっても認証処理にかかる時間を削減したい使用者や、認証処理にかかる時間や手間が増大してもセキュリティを確保したい使用者等に対して、適切なサービスを提供することができる。

さらに、複数の認証レベルを用意し、認証レベルが高い場合に保険額を低く設定したことにより、サイトにおける多様なサービスの提供と、より高い

認証レベルへの使用者の移行促進を両立することができる。また、認証代行サービス提供事業者にとっては、低い認証レベルでサービスを提供することのリスクを回避することができる。

5 また、本実施形態では、全体認証情報のみならず、携帯電話機の電話番号をも全体認証の必須要素としたことにより、使用者の正当性のみならず、使用者と携帯電話機との組み合わせの正当性をも認証することができる。特に携帯電話機は使用者に携帯されるものであるため、使用者の行動を制約することなく、高い精度で全体認証を行うことができる。

10 また、本実施形態では、サイトのシステムに変更を加えることなく、端末装置からサイトを利用する会員に、容易かつ安全に利用することができる認証サービスを提供する事を可能とし、サービスの提供価値を向上することができる。また、使用者においては、多様なサービスを容易かつ安全に利用できることになるから、認証を要する会員制サービスの利用意欲の向上を期待できる。

15

産業上の利用可能性

本発明は、認証情報の入力に要するサイトが提供するサービスの利用意欲を向上させることができる認証システム、ならびに当該認証システムを構成する認証代行装置および端末装置を提供する。

20

請 求 の 範 囲

1. 通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を
5 介して接続できる複数の端末装置と、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して
格納した第1のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使
用者固有の情報の少なくとも一方を利用して認証する第1の手段と、

10 第1の手段により認証された使用者が利用を希望するサイトを特定する第
2の手段と、

第1のデータベースを参照して、第1の手段により認証された前記使用者
と第2の手段により特定されたサイトとに対応した個別認証情報を抽出して、
当該サイトに抽出された第1の情報を渡す第3の手段とを有し、前記通信網

15 に接続した

認証代行装置と

を有する認証処理システム。

2. 前記端末装置が生体に固有な情報を取得する第4の手段を有し、当該生体
20 に固有な情報を使用して前記端末装置の使用者を認証することを特徴とする
請求項1に記載の認証処理システム。

3. 前記生体に固有な情報が指紋情報および声紋情報を含むことを特徴とす
る請求項2に記載の認証処理システム。

25

4. 前記生体に固有な情報が指紋情報を含むことを特徴とする請求項2に記
載の認証処理システム。

5. 前記生体に固有な情報が声紋情報を含むことを特徴とする請求項2に記

載の認証処理システム。

6. 前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項 1 に記載の認証処理システム。

5

7. 通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

10 前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第 1 のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第 1 の手段と、

第 1 の手段により認証された使用者が利用を希望するサイトを特定する第 2 の手段と、

15 第 1 のデータベースを参照して、第 1 の手段により認証された前記使用者と第 2 の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第 1 の情報を渡す第 3 の手段と

前記第 1 の手段が複数の認証レベルを備え、前記使用者が当該認証レベルを選択することを可能とする第 5 の手段と

20 を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

25 8. 前記端末装置が当該生体に固有な情報を取得する第 4 の手段を有し、前記第 1 の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを特徴とする請求項 7 に記載の認証処理システム。

9. 前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項 7 に記載の認証処理システム。

1 0 . 通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

5 前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第 1 のデータベースと、

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第 1 の手段と、

10 第 1 の手段により認証された使用者が利用を希望するサイトを特定する第 2 の手段と、

第 1 のデータベースを参照して、第 1 の手段により認証された前記使用者と第 2 の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第 1 の情報を渡す第 3 の手段と、

15 前記第 1 の手段で前記使用者が認証レベルを選択することを可能とする第 5 の手段と、

前記第 5 の手段により前期認証レベルに基づいて、当該使用者に対する保険料を請求する手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

20

1 1 . 前記端末装置が当該生体に固有な情報を取得する第 4 の手段を有し、前記第 1 の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを可能とすることを特徴とする請求項 1 0 に記載の認証処理システム。

25

1 2 . 前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項 1 0 に記載の認証処理システム。

1 3 . 通信網と、

前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記複数のサイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第 1 のデータベースと、

- 5 前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第 1 の手段と、

第 1 の手段により認証された使用者が利用を希望するサイトを特定する第 2 の手段と、

- 10 第 1 のデータベースを参照して、第 1 の手段により認証された前記使用者と第 2 の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第 1 の情報を渡す第 3 の手段と、

第 1 の手段によって認証される認証の効果の有効期限を管理する第 7 の手段とを有し、前記移動網に接続した

認証代行装置と

- 15 を有する認証処理システム。

- 1 4. 前記端末装置が当該生体に固有な情報を取得する第 4 の手段を有し、前記第 1 の手段が当該生体に固有な情報を含む情報を使用して前記端末装置の使用者を認証することを可能とすることを特徴とする請求項 1 3 に記載の認証処理システム。
- 20

1 5. 前記端末装置に固定された情報が当該端末装置の電話番号であることを特徴とする請求項 1 3 に記載の認証処理システム。

- 25 1 6. 通信網と、

生体に固有の情報を含む情報を取得する第 4 の手段と、取得した生体に固有の情報を認証前段処理する第 8 の手段とを有し、前記通信網に通信手段を介して接続できる複数の端末装置と、

前記通信網に接続した複数のサイトと、

前記端末装置の使用者を、前記第 8 の処理で処理された情報を利用して認証する第 9 の手段と、

前記複数のサイトに対応した複数の個別認証情報を、前記使用者に対応して格納した第 1 のデータベースと、

5 前記第 9 の手段により認証された使用者が利用を希望するサイトを特定する第 2 の手段と、

前記第 1 のデータベースを参照して、前記第 9 の手段により認証された前記使用者と前記第 2 の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された個別認証情報を渡す第 3 の手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

1 7. 通信網と、

15 前記通信網に通信手段を介して接続できて、複数のサイトに前記通信網を介して接続できる複数の端末装置と、

前記複数のサイトに入力する個別認証情報を、前記端末装置の使用者に对应して格納した第 1 のデータベースと、

20 前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第 1 の手段と、

第 1 の手段により認証された使用者が利用を希望するサイトを特定する第 2 の手段と、

第 1 のデータベースを参照して、第 1 の手段により認証された前記使用者と第 2 の手段により特定されたサイトとに対応した個別認証情報を抽出して、当該サイトに抽出された第 1 の情報を渡す第 3 の手段と、

25 前記第 2 のデータベースを、前記複数のサイトが更新することを可能とする第 1 0 手段を有し、前記通信網に接続した

認証代行装置と

を有する認証処理システム。

1 8. 複数の端末装置と通信網を介して接続できて、複数のサイトに通信網を介して接続できて、

前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して
5 格納した第1のデータベースと、

前記個別認証情報の種類と属性を含むサイト情報を、当該サイトに対応して格納した第2のデータベースと

前記端末装置の使用者を、当該端末装置に固定された情報あるいは当該使用者固有の情報の少なくとも一方を利用して認証する第1の手段と、

10 第1の手段により認証された使用者が利用を希望するサイトを特定する第2の手段と、

前記第1のデータベースを参照して、前記第1の手段により認証された前記使用者と前記第2の手段により特定されたサイトとに対応した第1の情報を抽出して、当該サイトに抽出された第1の情報を渡す第3の手段とを有する
15

認証代行装置。

1 9. 複数の端末装置と通信網を介して接続できて、

複数のサイトに通信網を介して接続できて、

20 前記サイトに入力する個別認証情報を、前記端末装置の使用者に対応して格納した第1のデータベースと、

前記個別認証情報の種類と属性を含むサイト情報を、当該サイトに対応して格納した第2のデータベースと

前記端末装置の使用者を、当該所有者に固有の生体情報を利用して認証する第1の手段と、
25

第1の手段により認証された使用者が利用を希望するサイトを特定する第2の手段と、

前記第1のデータベースを参照して、前記第1の手段により認証された前記使用者と前記第2の手段により特定されたサイトとに対応した第1の情報

を抽出して、当該サイトに抽出された第 1 の情報を渡す第 3 の手段とを有する

認証代行装置。

5 20. 通信網に接続することができる通信手段と、

前記通信網を介してサイトおよび認証代行装置に接続することができる接続手段と、

生体に固有な情報を取得する第 4 の手段と、

前記取得した生体に固有な情報を認証前段処理する第 8 の手段とを有する

10 端末装置。

図 1

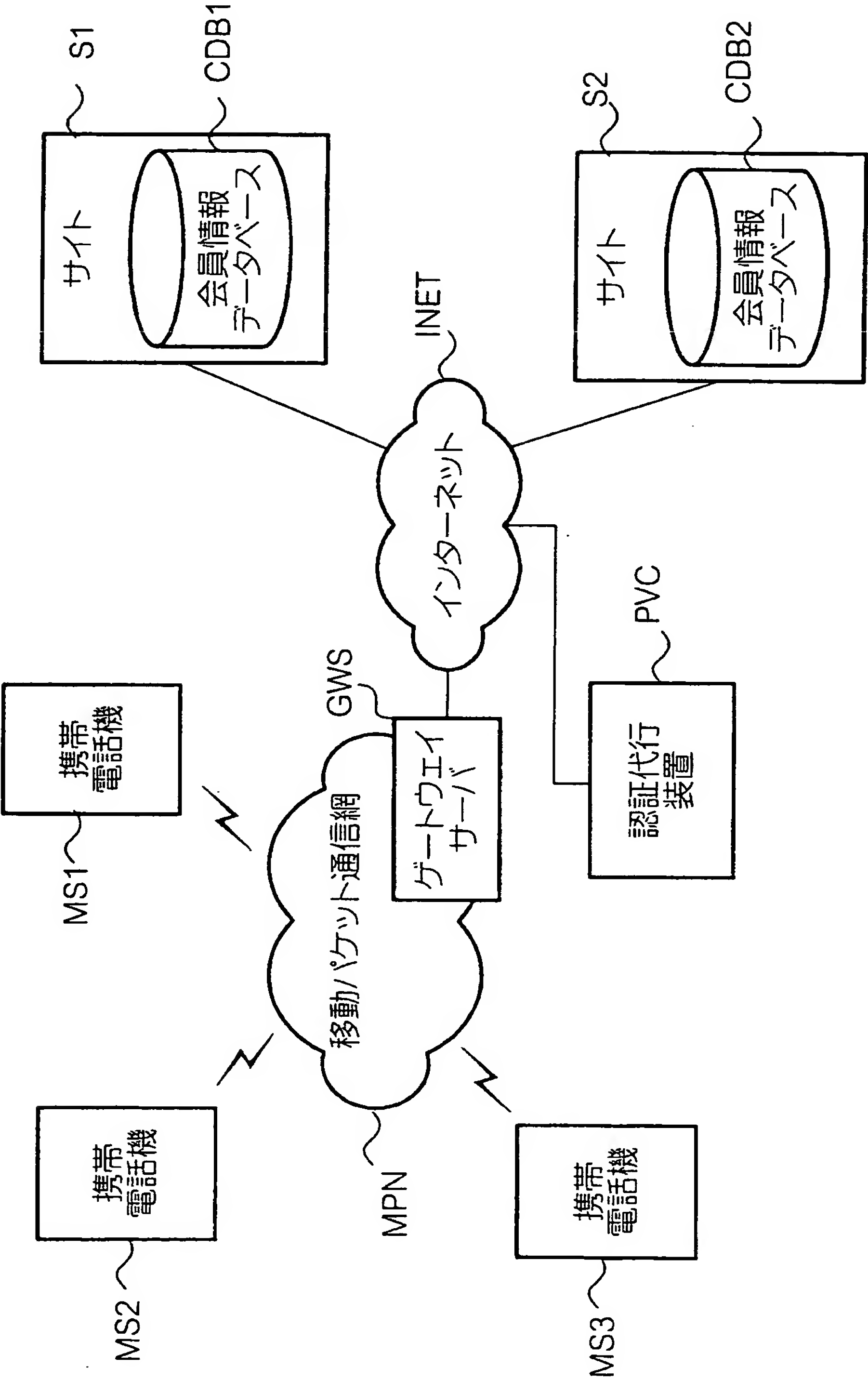


図 2

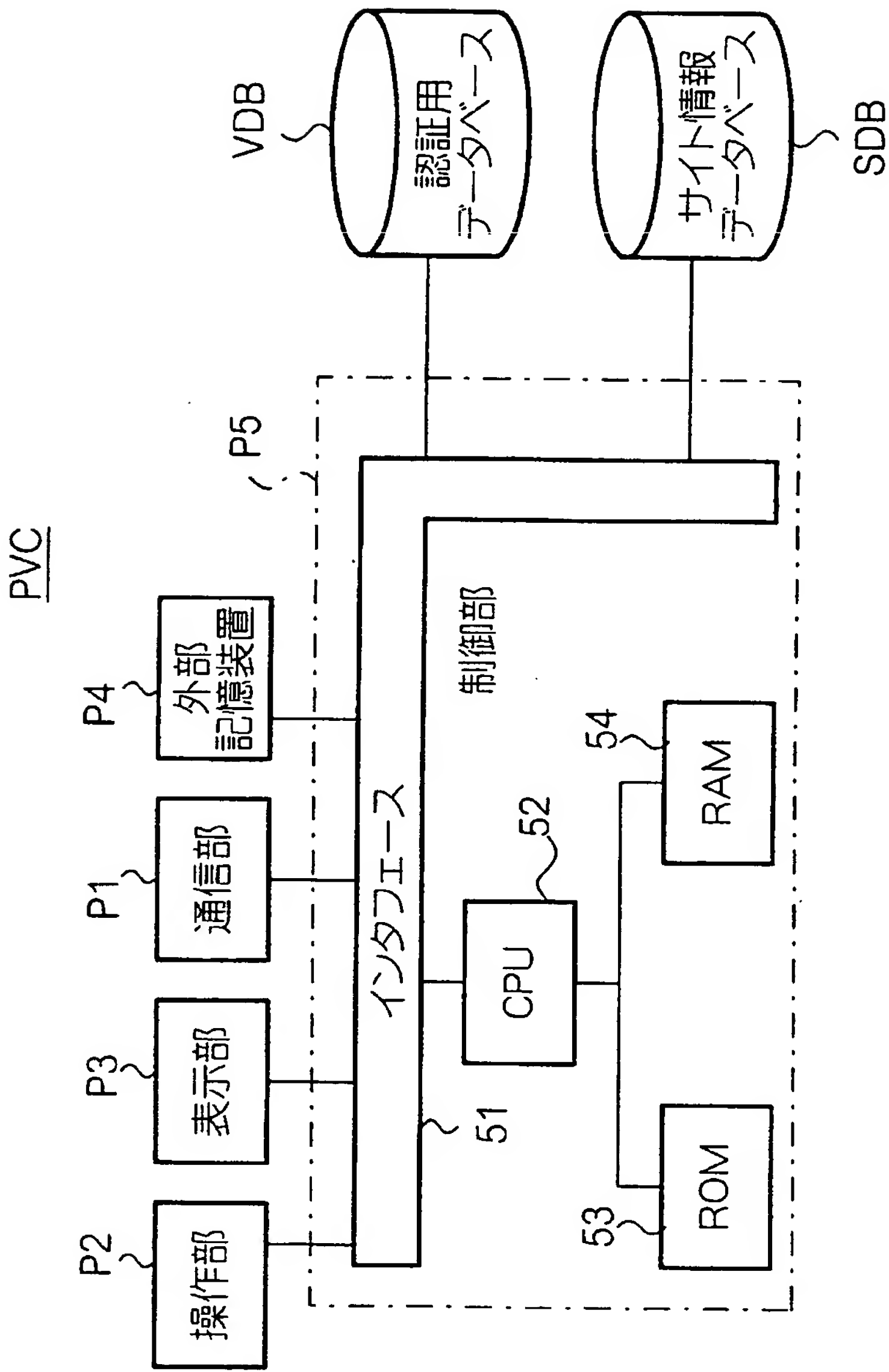


図 3

T1

会員 番号	名前	電話 番号	全体認証情報		認証 レベル	有効 期限	接続先 ID	個別認証情報		保険料	使用料
			声紋情報	指紋情報				ID	パスワード		
1	C	2	...	7	docom	*****	0	100
							5	omocod	—		
2	B	—	1	...	5	65883	—	100	100
3	A	—	1	100	100

図 4

T2

接続先 ID	タイトル	接続情報	分類	ID 要否	パスワード 要否	ID 属性	パスワード 属性
1	
2	
3	
4	
5	懸賞リスト	http://www.d.net/list/list.cgi	懸賞	要	否	4-8	...
6	
7	D社ポイント	https://www.c.co.jp/point/point.cgi	ショッピング	要	要	4-8	8-16
8	

図 5

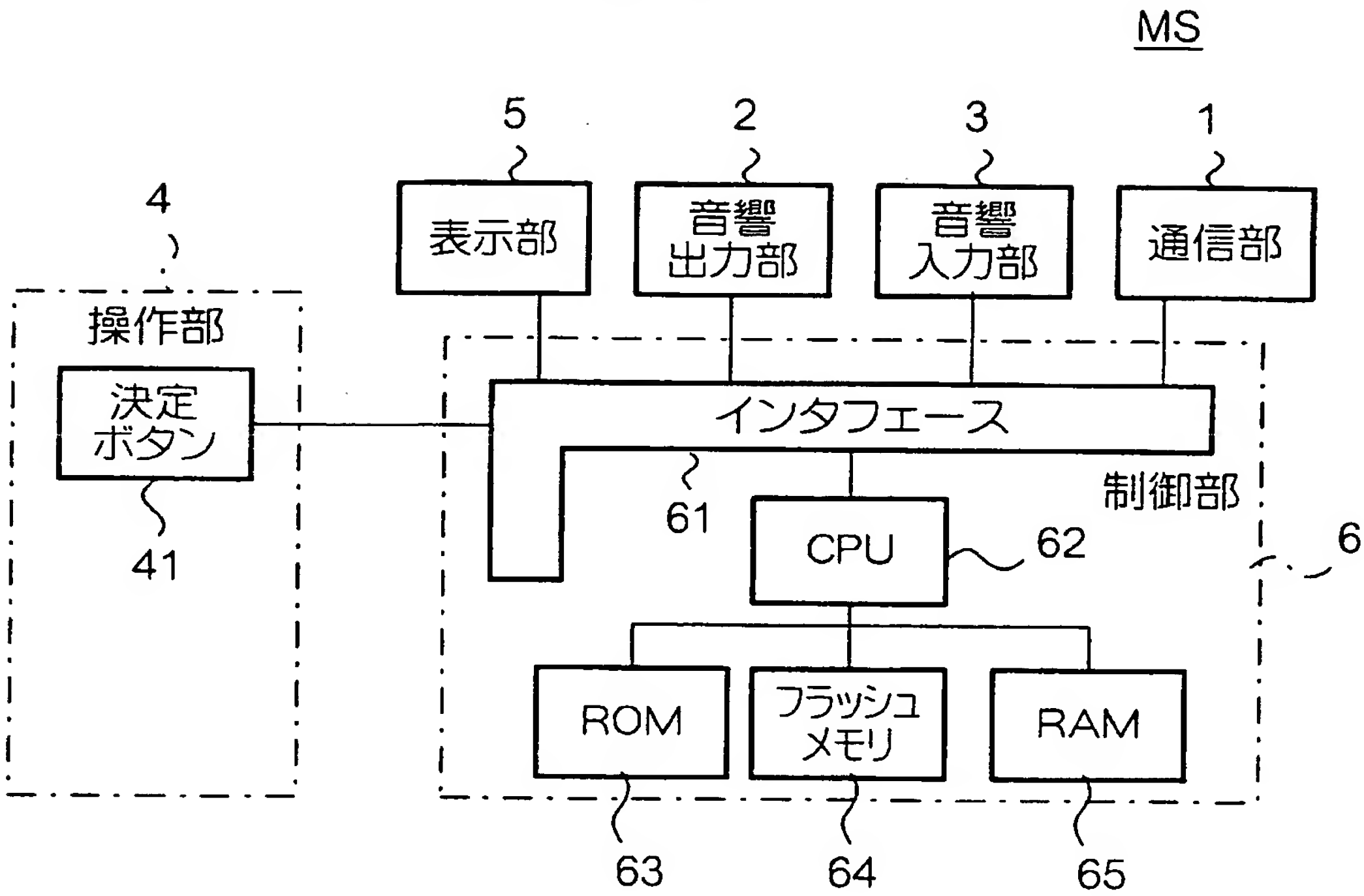
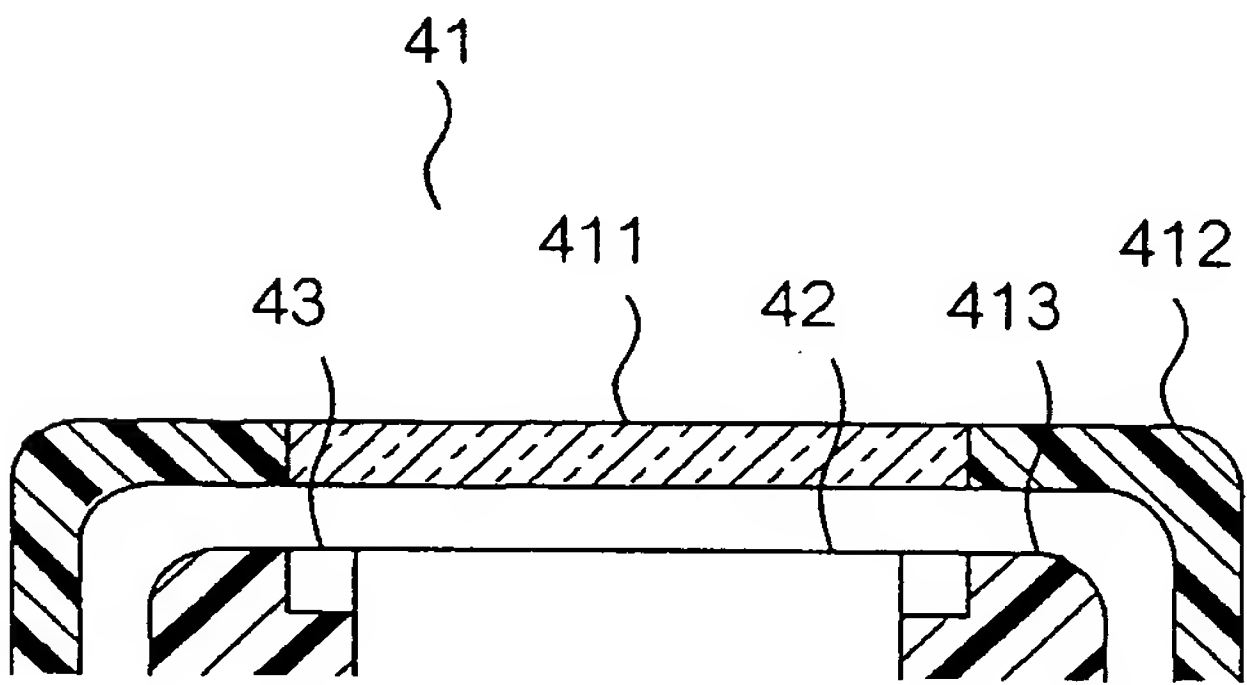


図 6



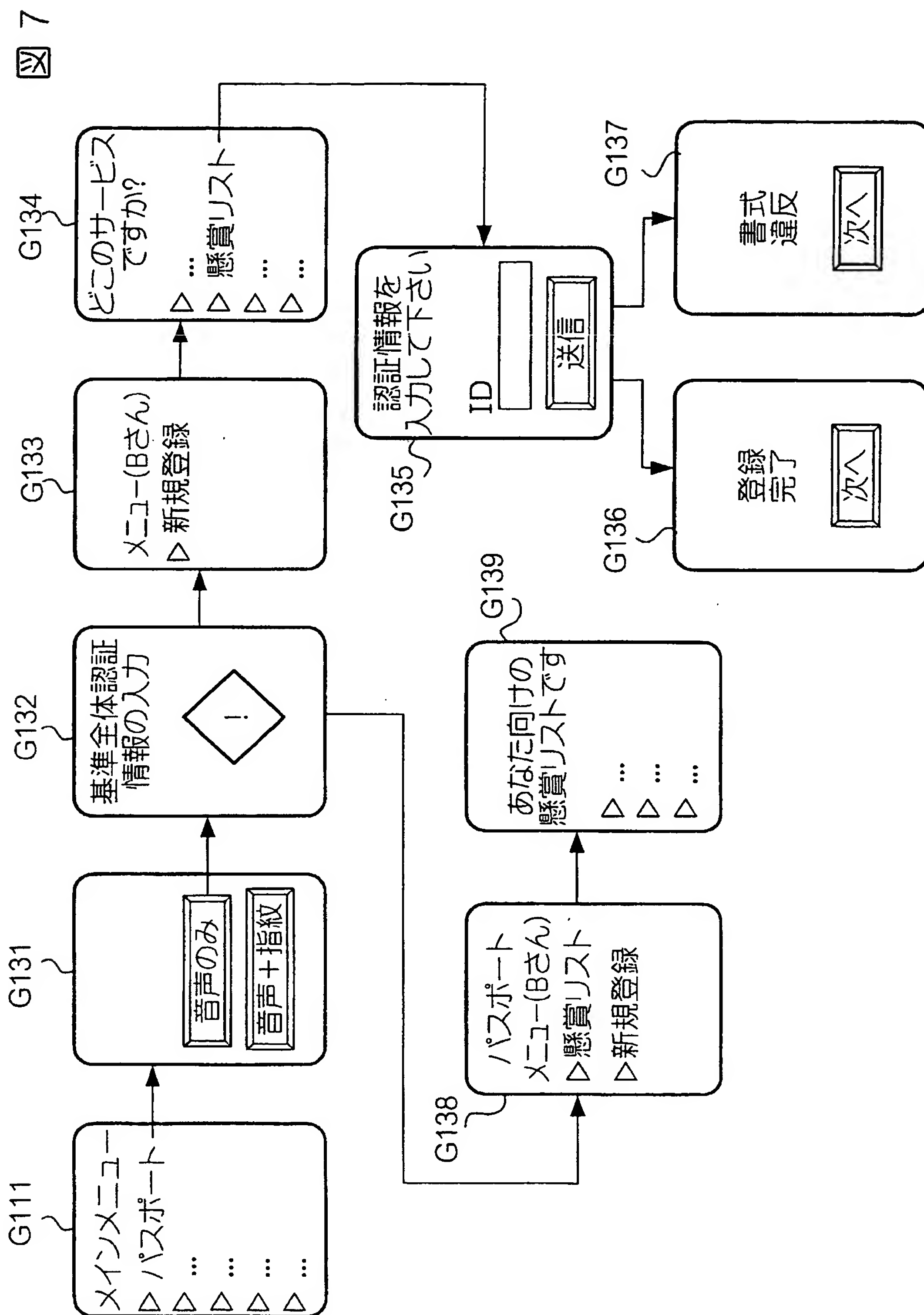


図 8

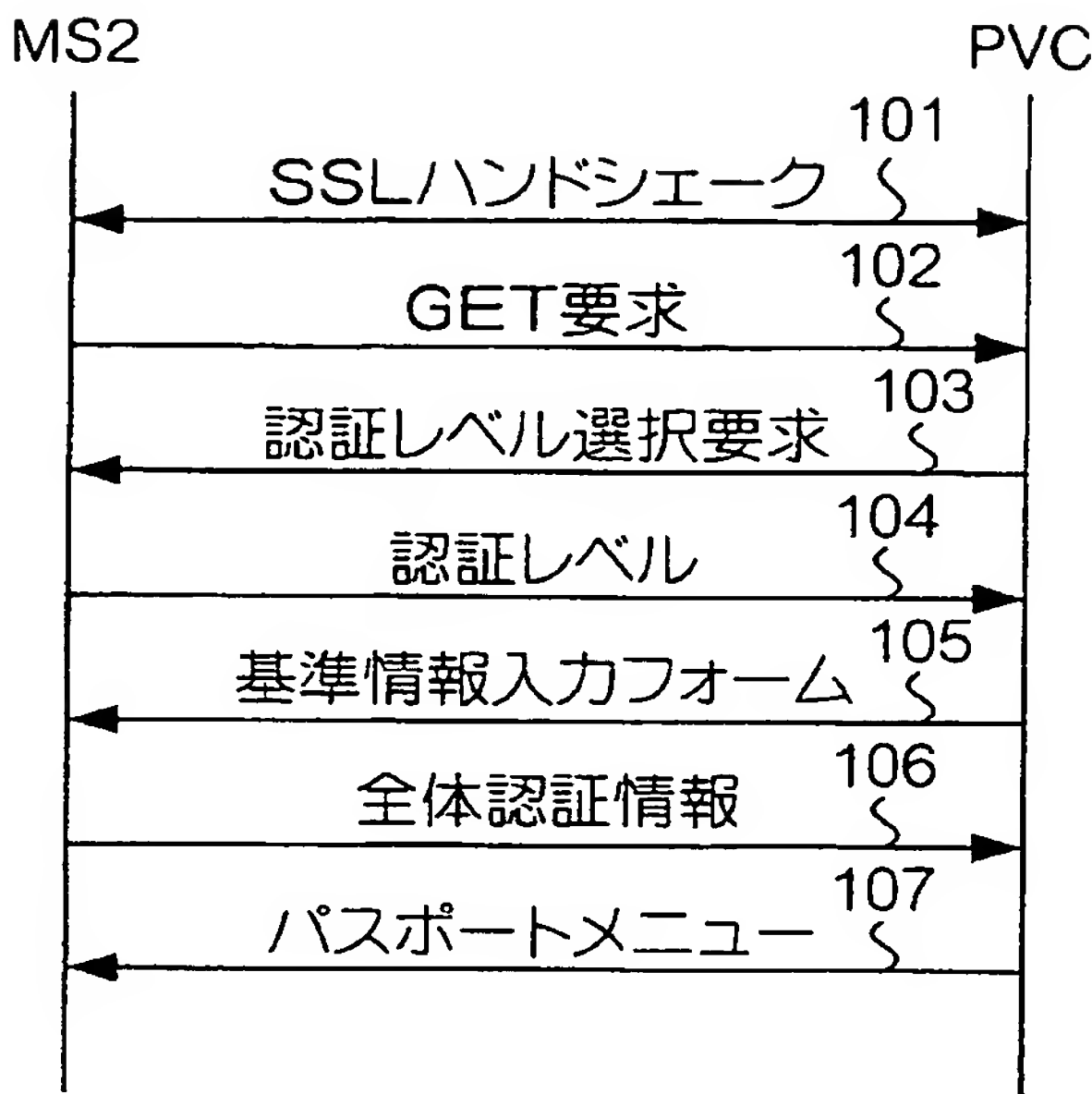


図 9

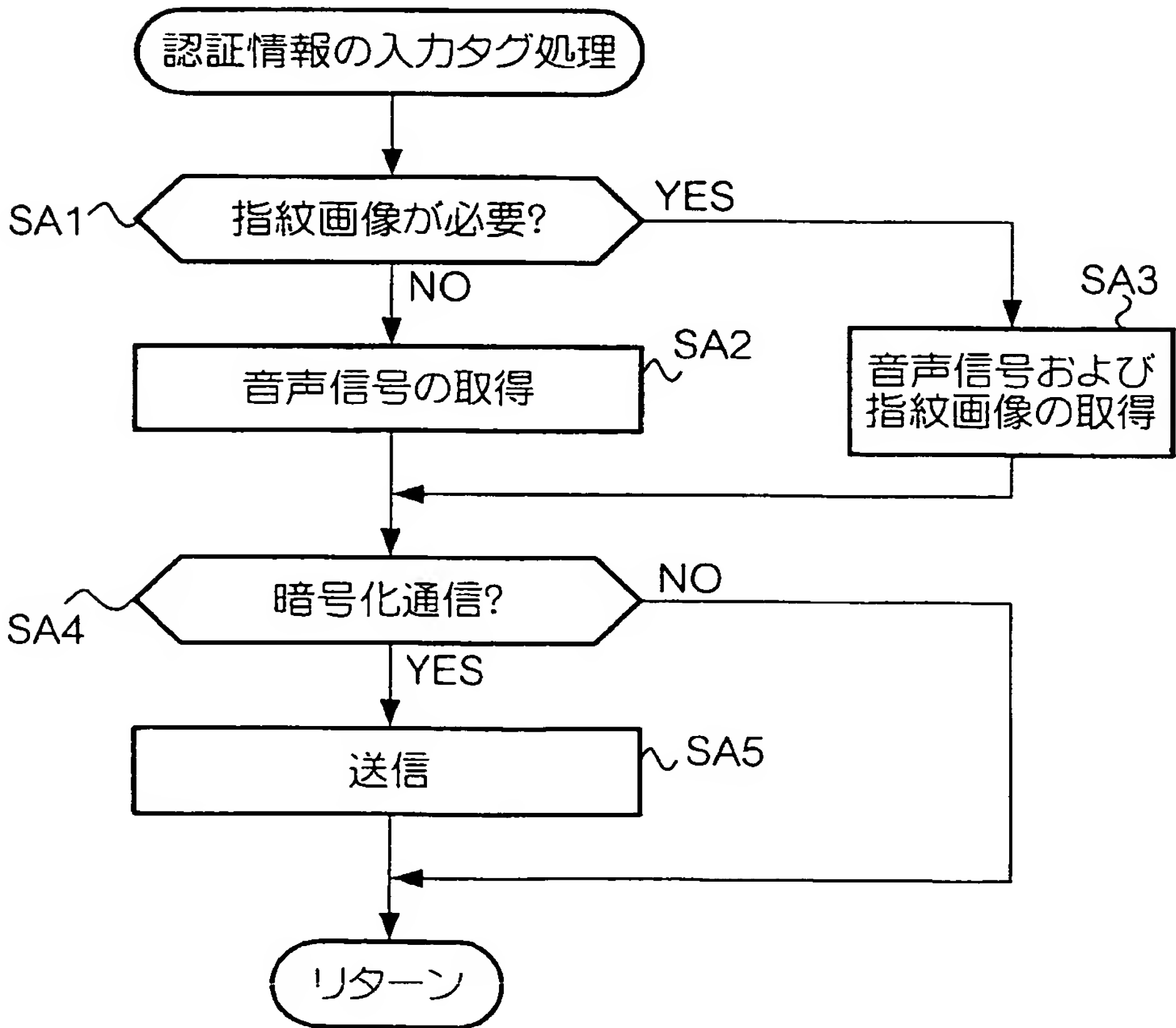


図 10

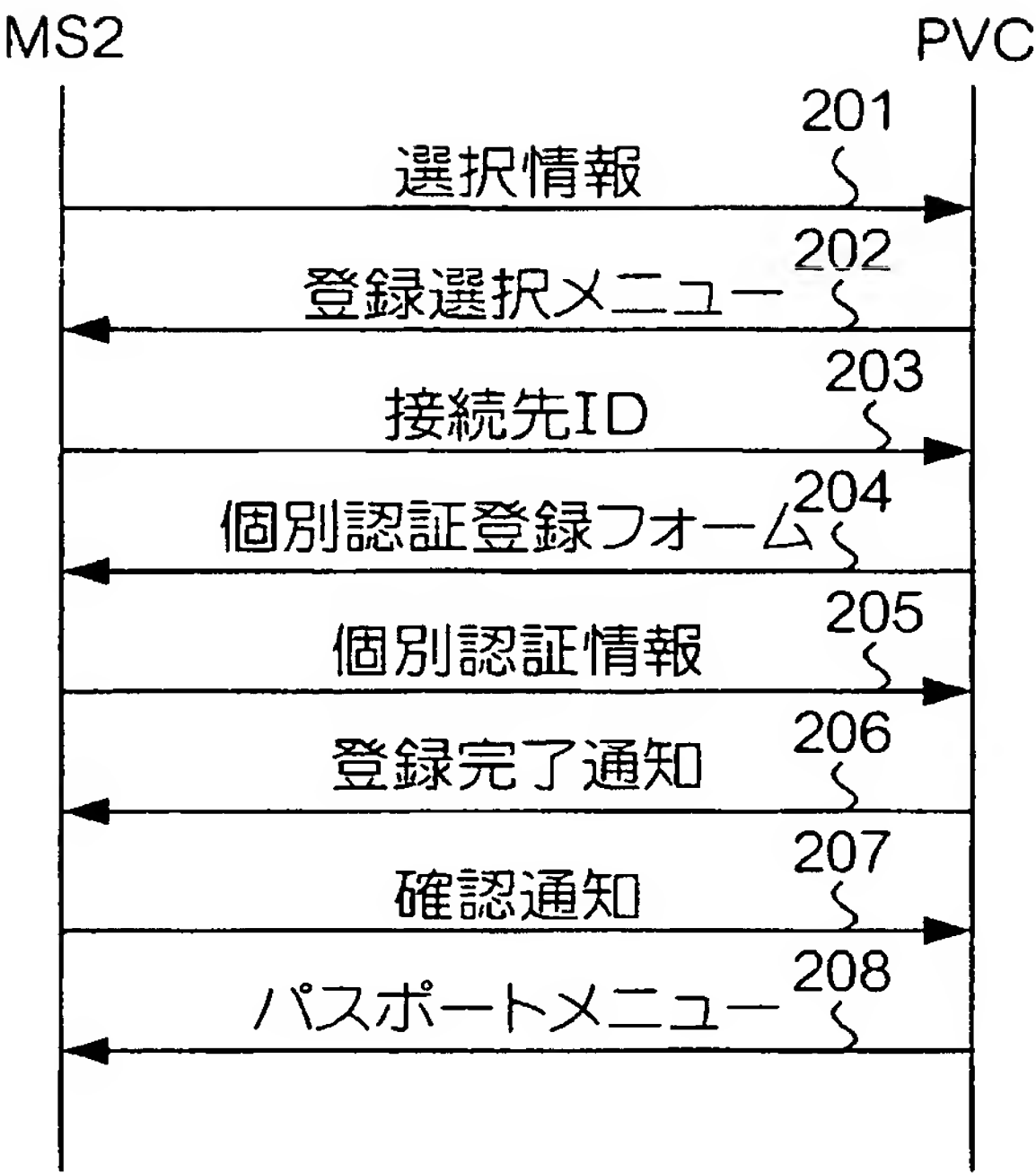


図 11

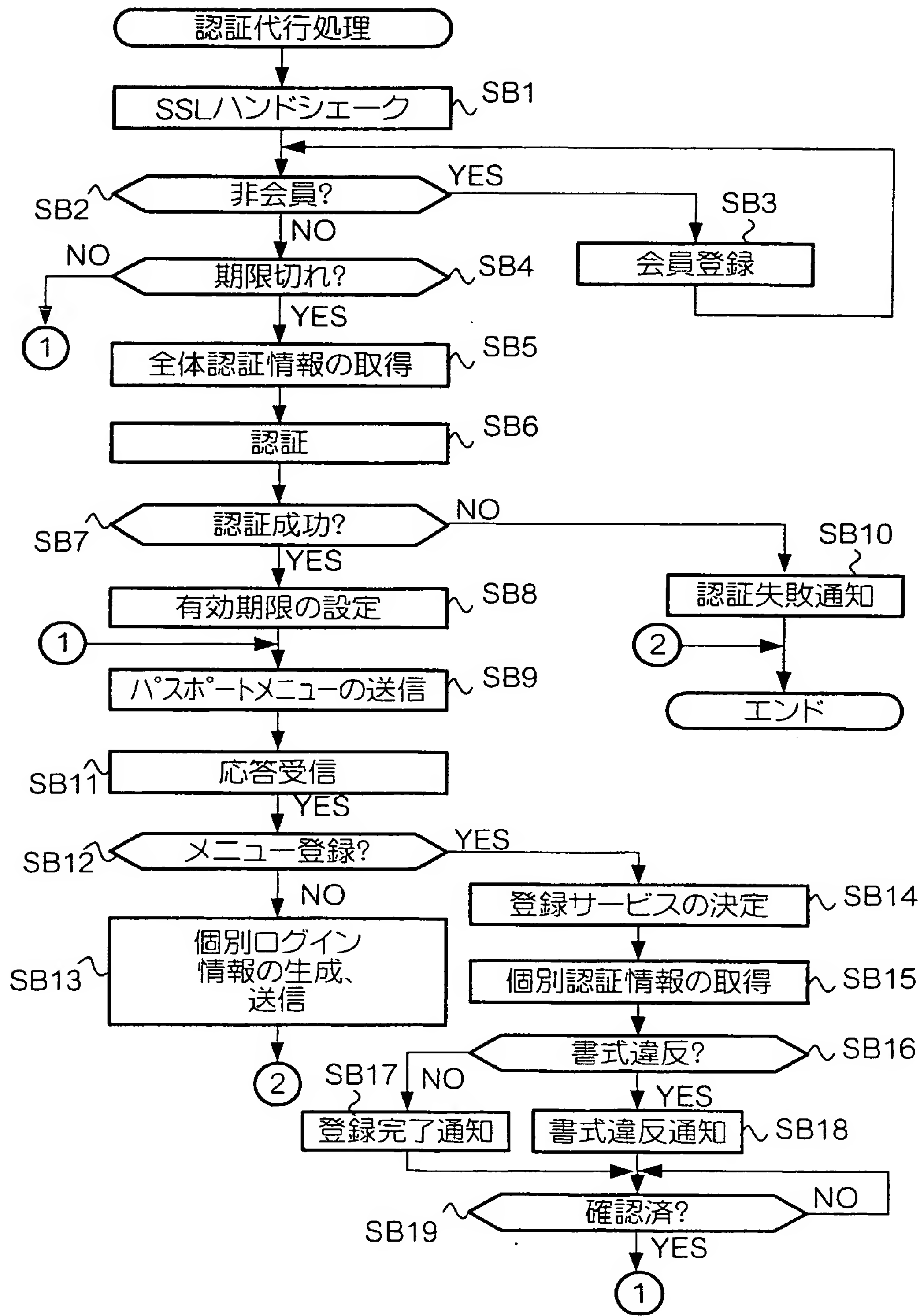


図 12

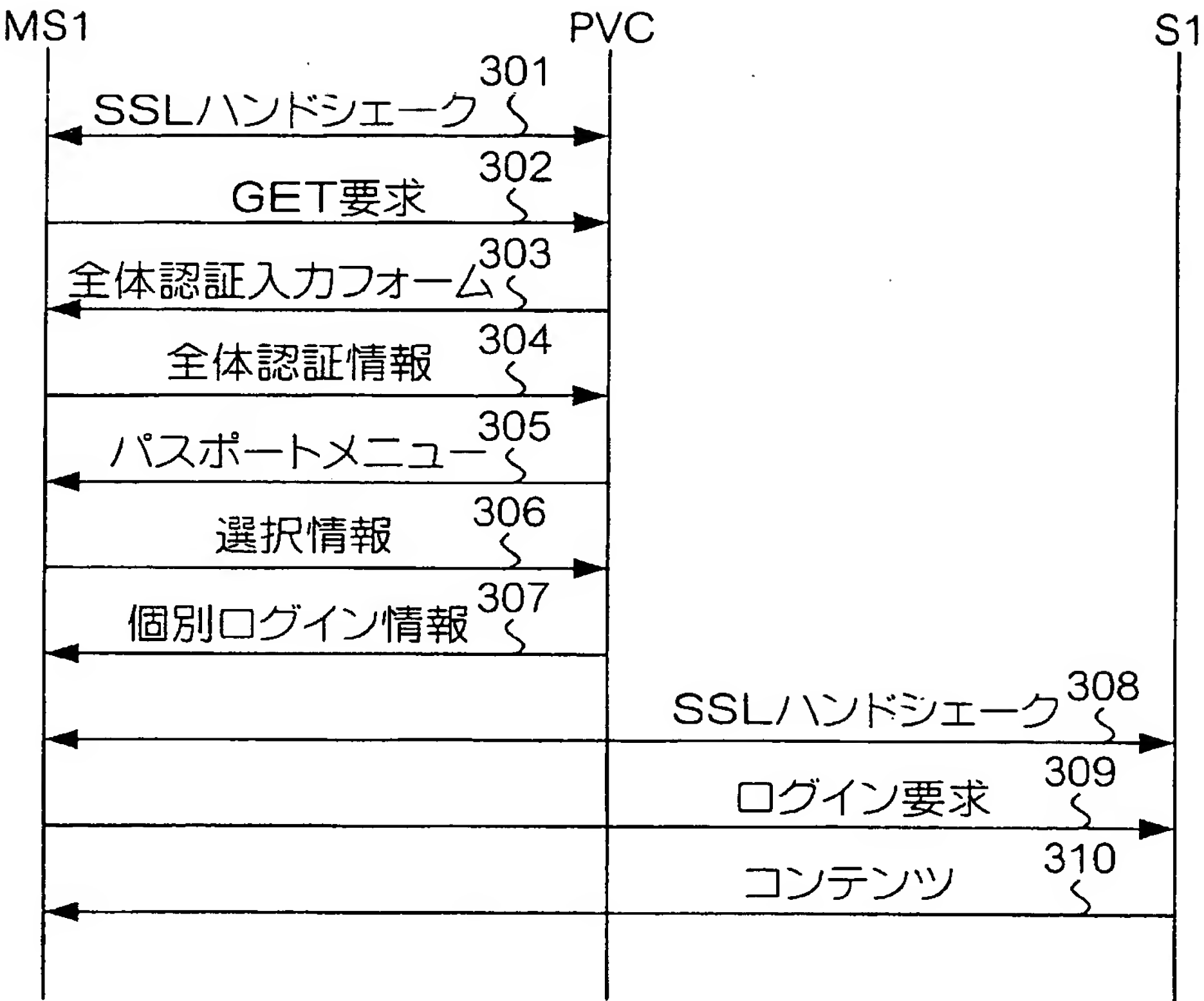


図 13

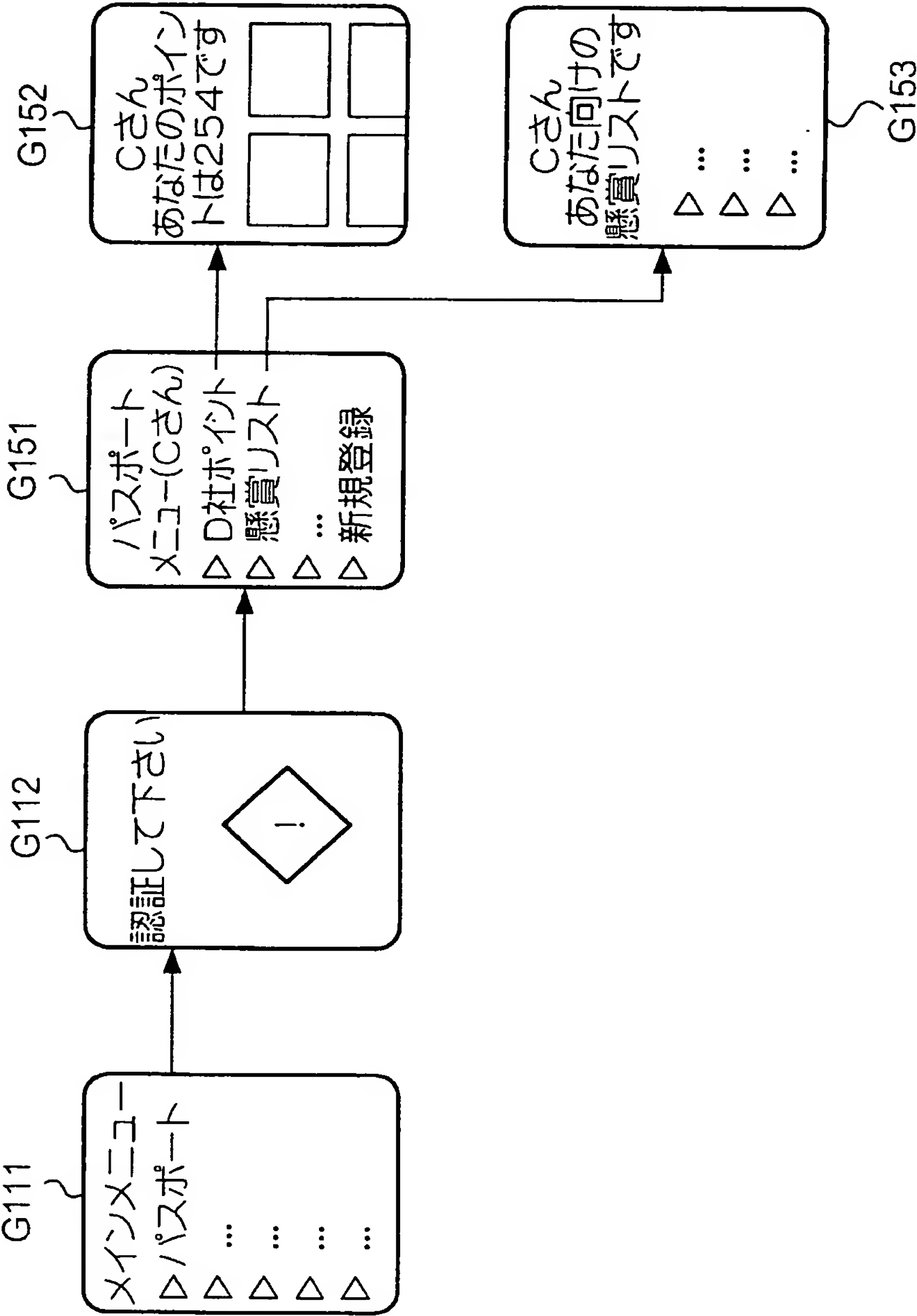


図 14

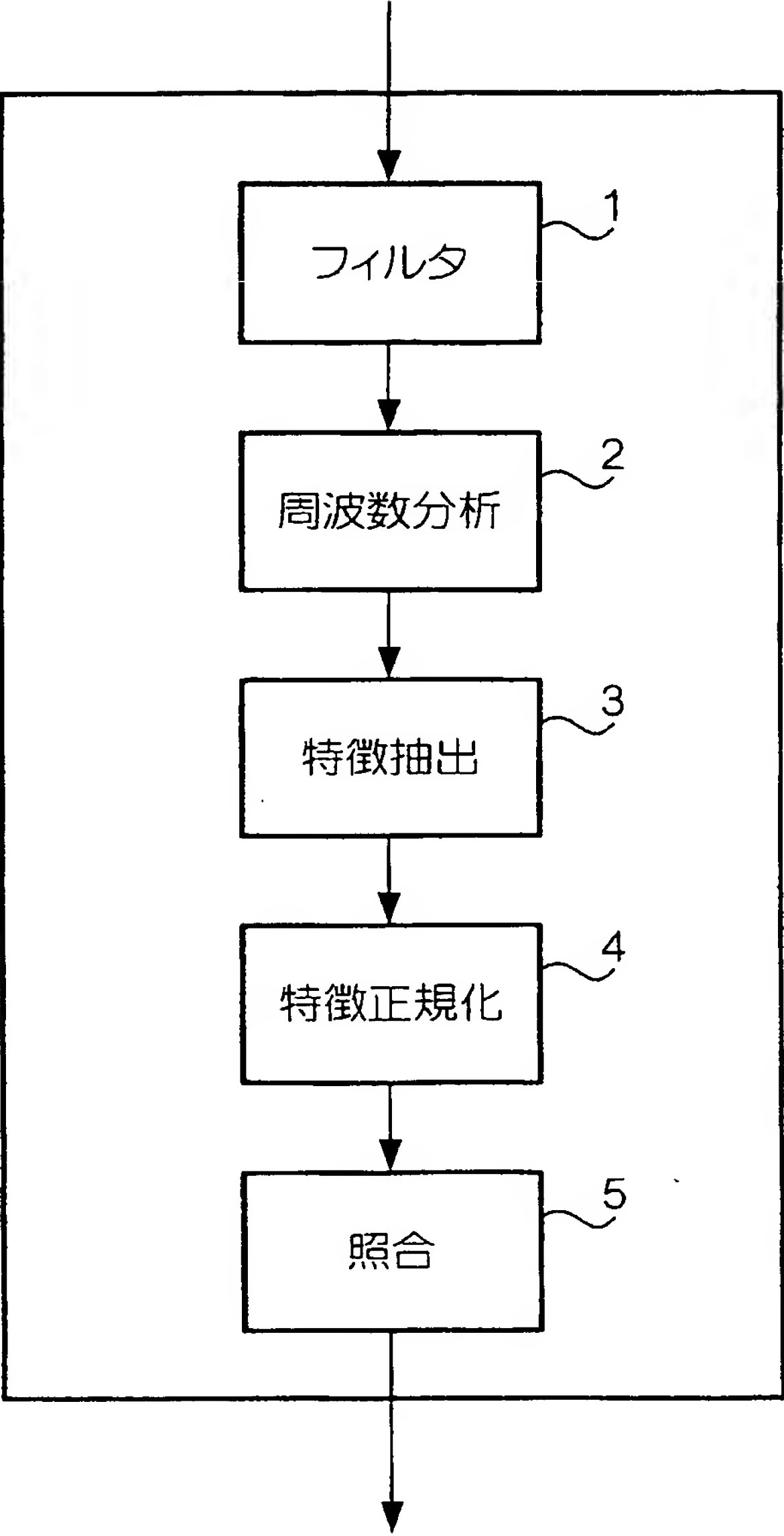


図 15

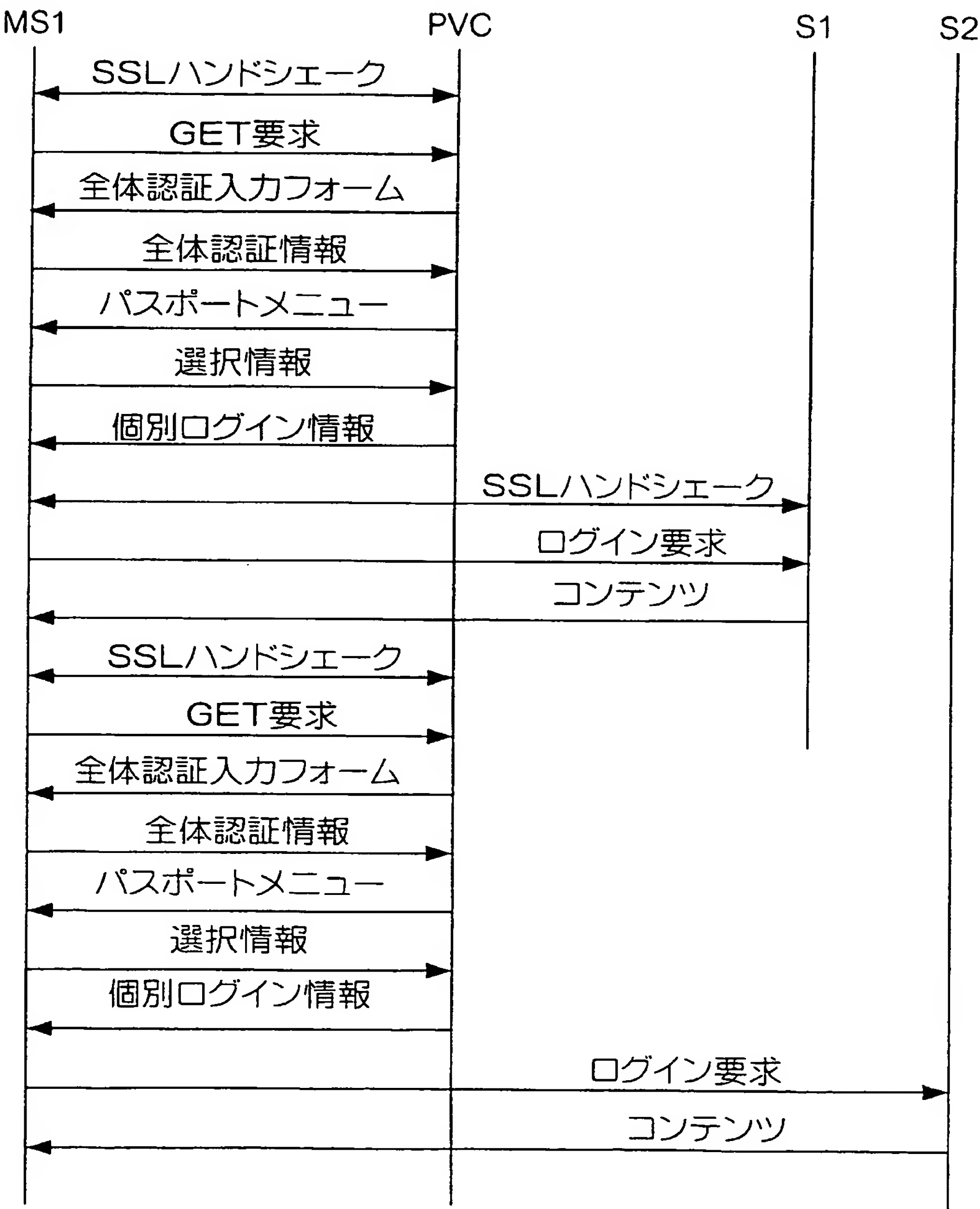


図 16

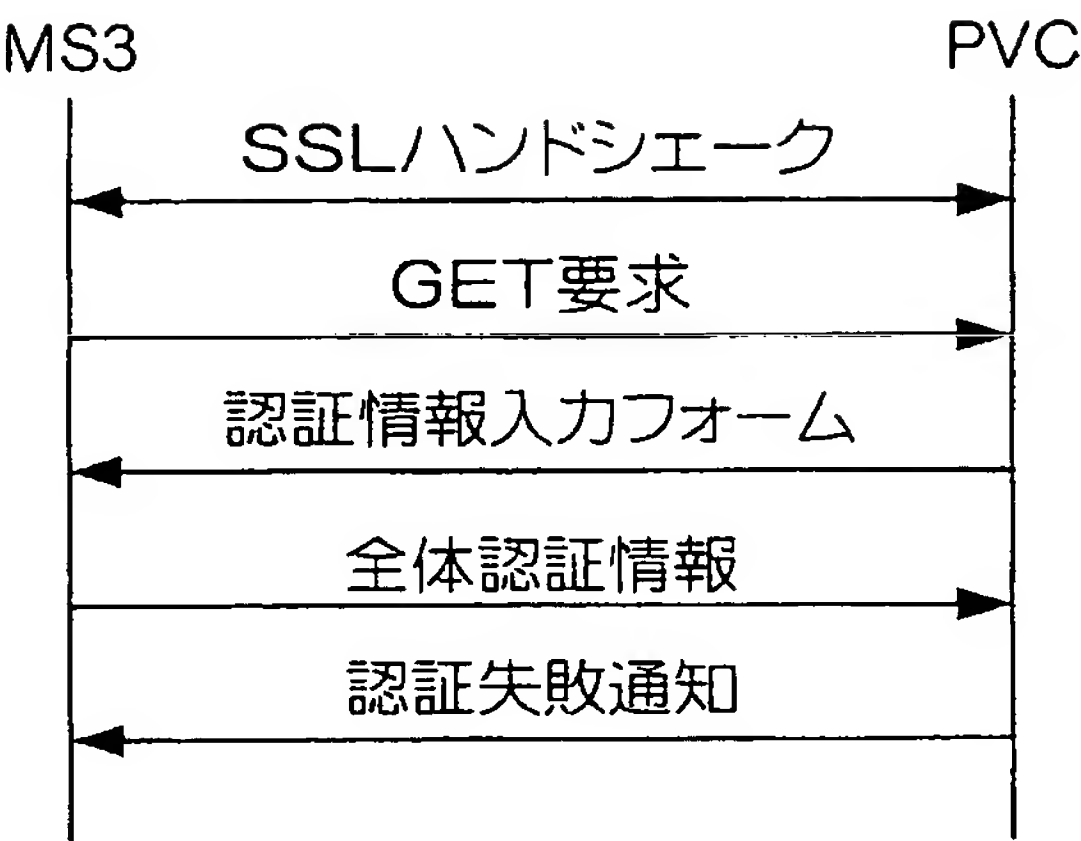


図 17

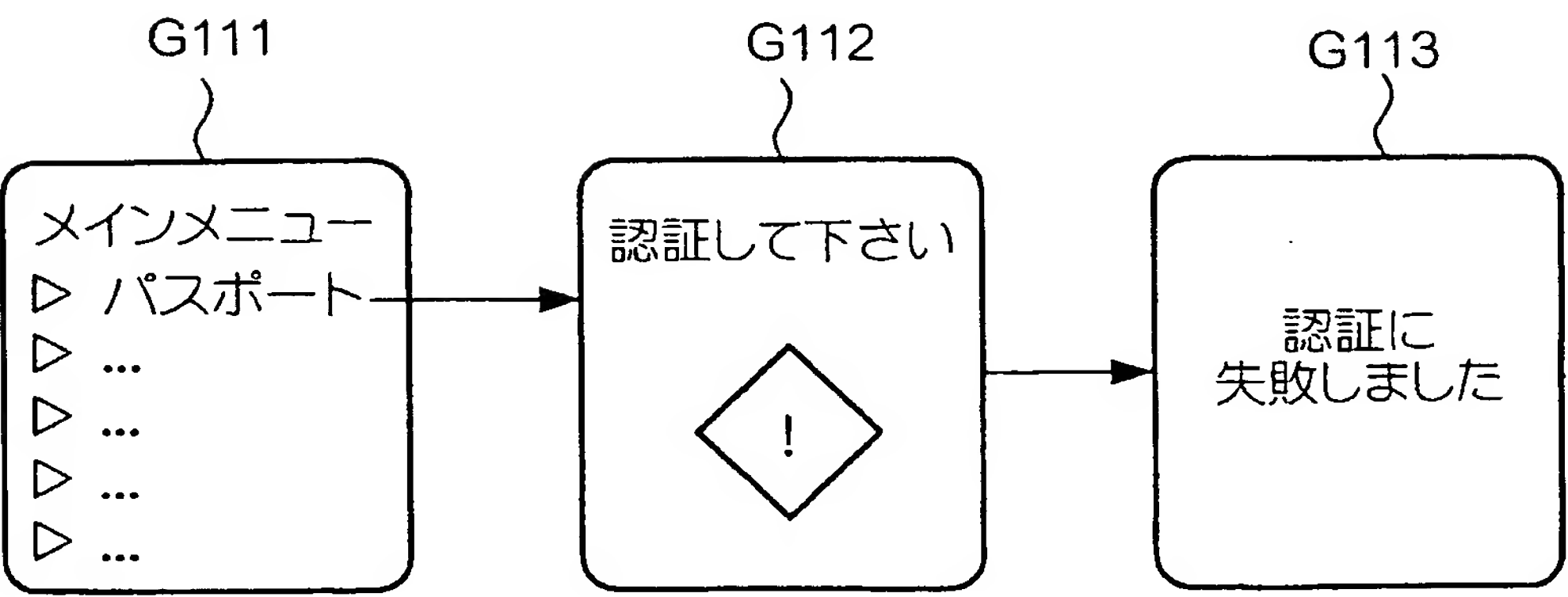
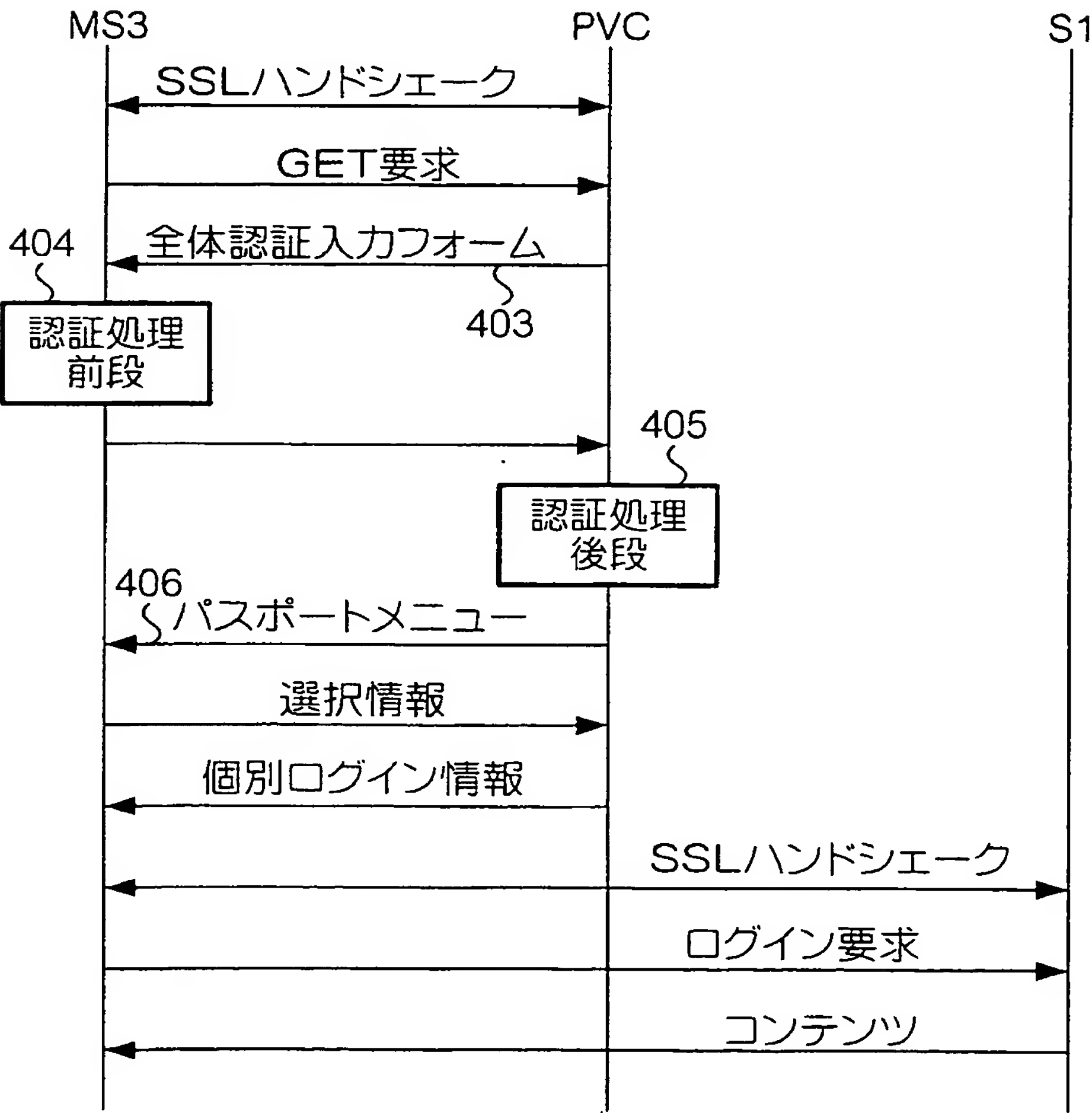


図 18

認証レベル	照合情報	保険料
1	音声信号	100
2	指紋画像	50
3	指紋画像および 音声信号	0

図 19



THIS PAGE BLANK (USP 10)